PREVENTING FRAUD AND IDENTITY THEFT
SDPD Neighborhood Policing Resource Team
April 19, 2012

CONTENTS

Fraudulent Checks
Free Samples
Gift Card Stripping
Green Dot Moneypaks
Green Energy Conservation
Healthcare Fraud
High-Pressure Sales of Financial Products At Free-Meal Seminars
Immigration Services
Investment Opportunities
Job Offers
Landlord Impersonation
Medicare Enrollment
Post-Foreclosure Solicitations
Predatory Insurance Sales Practices
Prize Notification and Lotteries
Property Tax Relief
Reverse Mortgages
Short Sales of Homes
Tax Debt Relief
Third-Party Telephone Bill Charges
Timeshare Transactions
Unscrupulous Contractors.

SAFER USE OF THE INTERNET

This paper contains tips for preventing telemarketing fraud, Internet fraud and other crimes, identity theft, Wi-Fi hacking and hotspot dangers, and other scams. It also contains tips and advice for safer use of the Internet. Many of these tips also apply to text messaging.

Additional tips on personal safety and security, home and vehicle security, vacation safety and security, senior safety and security, preventing crimes against businesses, reporting crime and suspicious activities, reporting suspicious activities for terrorism prevention, reporting disorder and other problems, obtaining crime information, dealing with homeless people, and starting a Neighborhood Watch program can be found on the SDPD website at **www.sandiego.gov/police**.

TELEMARKETING FRAUD

Callers claiming to represent everyone from police officers to the disabled take advantage of the public's sympathy and generosity to the tune of billions of dollars each year. They also offer miracle cures for everything from baldness to cancer, vacation time shares, sweepstakes prizes, chances to earn enormous profits from no-risk, high-yield business and investment opportunities, etc. Be suspicious of all solicitors, especially if the caller:

- Says you have won a prize or lottery but asks you to send money first or provide bank account information.
- Says you have to act right away. Remember, if it's a good deal today it will still be a good deal tomorrow. Don't let anyone rush you into signing anything.
- Fails to identify the sponsor, uses a variation of an official or nationally-recognized name, e.g., Salvation League instead of Salvation Army.
- Offers to have someone pick up a cash payment from your home.
- Says he or she is a law enforcement officer who will help you for a fee.
- Requires you to attend a sales meeting.
- Directs you to dial a pay-per-call **900** number.
- Directs you to a strange area code, e.g., 876 which in Jamaica. In addition to soliciting money and personal information, these calls can be expensive with the cost being split between the phone company and the number owner. So the longer you talk, the more money the number owner gets. So never call back a number with an area code you don't recognize. You can get area-code locations online, e.g., at **www.areacodelocation.info/areacodelist.html**.
- Delays the delivery or a product or prize, etc.

- Says he or she is calling from the Security and Fraud Department of your credit- or debit-card company and asks you for the 3-digit security number on the back of your credit card to verify your possession of the card to aid it in a fraud investigation.
- Says that Medicare now requires a National ID Card and offers to provide one for a fee.
- Says he or she is a U.S. Food and Drug Administration (FDA) agent or official and that you must pay a fine because you have bought or attempted to buy discounted prescription drugs from a foreign pharmacy. Report such calls to the FDA Office of Criminal Investigations at **(800) 521-5783**.
- Says he or she is calling from Microsoft or some legitimate company to warn you that your computer has a security problem and offer a free security check. You may then be tricked into allowing access to your computer, downloading malware, i.e., malicious software of all kinds, giving out credit card information, or buying some software or services that you don't need. If you fall for this scam you should change all your computer and financial institution passwords, scan you computer for malware, and contact you bank and credit card providers.

Hang up immediately if the caller is rude or threatening. And report any threatening calls to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**.

The following tips will help you resist these criminal appeals.

- Never give your credit or debit card, checking account, Social Security or Medicare number, or any personal information to an unknown caller. Just say "no" and hang up on anyone who asks for personal information. Don't ever assume a friendly voice belongs to a friend.
- Never give out the 3-digit security number on the back of your credit or debit card unless you have initiated a card purchase and the seller asks for it to verify your possession of the card.
- Ask a charity to send written information about its finances and programs before making any commitments.
- Call the Better Business Bureau (BBB) of San Diego County at **(858) 496-2131** to check on any unsolicited offers. Or visit its website at **www.sandiego.bbb.org** to see whether the business is accredited. And for any business, you can check its rating, reason for the rating, and the number of closed complaints in five categories. Its website also has general consumer information and tips on avoiding various types of fraud.
- For additional information contact the Federal Trade Commission (FTC) Consumer Response Center at **(877) 382-4357** and **www.ftc.gov**, Federal Communications Commission Consumer Center at **(888) 225-5322** and **www.fcc.gov/ccb/consumer_news/**, and California Department of Consumer Affairs Consumer Information Center at **(800) 952-5210** and **www.dca.ca.gov/consumer/cic**.
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to check on any solicitations regarding Medicare.

And be sure to list your home and mobile phone numbers free on the National Do Not Call Registry to reduce pre-approved credit offers and telemarketing calls. Call **(888) 382-1222** or register online at **www.donotcall.gov**. Telemarketers check the registry every 31 days so it may take that long before your numbers are removed from their call lists. This should stop all but exempt calls from nonprofit groups, charities, political organizations, survey companies, and companies you have dealt with recently or signed a contract with that includes permission to call you. If telemarketers ignore the fact that your numbers are on the registry you can report them at the above number or website and sue them for violating your rights. For this you'll need to keep a record of their names and the dates of the calls. If you receive non-exempt recorded telemarketing solicitations known as robocalls, now banned by the FTC, you can file a complaint with the commission online at **www.ftc.gov** or by phone at **(877) 382-4357**.

INTERNET FRAUD AND OTHER CRIMES

In 2009 the Internet Crime Complaint Center (IC3), which acts in partnership with the National White Collar Crime Center and the FBI, received more than 336,000 complaints on its website and referred over 146,000 to law enforcement agencies for further consideration. The total loss from all of these cases was over $560 million. You may be at risk if you answer "yes" to any of the following questions:

- Do you visit websites by clicking on links within an e-mail?
- Do you reply to e-mails from persons or businesses you are not familiar with?
- Have you received packages to hold or ship to someone you met on the Internet?

- Have you been asked to cash checks and wire funds to someone you met on the Internet?
- Would you cash checks or money orders received through an Internet transaction without first confirming their legitimacy?
- Would you provide your personal banking information in response to an e-mail notification?

If you become a victim of Internet fraud or receive any suspicious e-mails you should file a complaint with the IC3 at **www.ic3.gov**. Its website also includes tips to assist you avoiding a variety of Internet frauds. You should also contact your e-mail provider. Most keep track of scams. Send your provider the suspicious message header and complete text. For more information on Internet fraud visit **www.LooksTooGoodToBeTrue.com**.

The following material deals with several specific kinds on Internet fraud and other crimes: e-mail scams and malware, online shopping frauds, phishing, spear phishing, smishing, vishing, whaling, social network dangers, illegitimate websites, e-card dangers, and unsafe drugs from online pharmacies.

E-mail Scams and Malware

Cybercriminals use e-mail in many clever ways to try to take your money and identity, and disrupt your computer operation, gather sensitive information, or gain unauthorized access to your computer. To protect your assets and computer you should never reply, click on any links, or open any attachments of e-mails that offer great bargains or something that's not legal. And if you don't recognize the sender, you should delete the e-mail without even opening it. Be especially suspicious about the following:

- Business opportunities to make money with little effort or cash outlay
- Offers to sell lists of e-mail addresses or software
- Chain letters involving money
- Work-at-home schemes
- Health and diet claims of scientific breakthroughs, miraculous cures, etc.
- Get-rich-quick schemes
- Free goods offered to fee-paying group members
- Investments promising high rates of return with no risk
- Kits to unscramble cable TV signals
- Guaranteed loans or credit on easy terms
- Credit repair schemes
- Vacation prize promotions
- Special offers that require a credit check and a small fee for verification expenses to be paid by a credit or debit card
- Notices of prize or lottery winnings that require you to pay a fee to cover expenses
- Requests for personal or financial information

Regarding the latter, cybercriminals often pose as government agencies or financial institutions that you normally deal with. Remember that government agencies never send important things by e-mail, and your financial institutions already have your personal information.

If you suspect something might be a scam, check it out on Hoaxslayer at **www.hoax-slayer.com**. This website is devoted to debunking e-mail hoaxes and exposing Internet scams. It is constantly increasing its compiled list of scams.

Online Shopping Frauds

Do not use a debit card when shopping online, especially on an unfamiliar website. If something goes wrong your account can be emptied quickly without your knowledge. This can result in overdrafts, fees, and an inability to pay your bills. Even if your bank offers a fraud guarantee it is not obligated to restore your funds for at least two weeks while it investigates. If have to use a debit card, use one that is reloadable. Then you only risk the amount you put on the card if something goes wrong.

If you use a credit card the federal Fair Credit Billing Act limits your liability to $50 for any unauthorized or fraudulent charges made before you report the billing error. To protect yourself you need to do the following:

- Write to your credit card company within 60 days after the date of the statement with the error and tell it your name and account number, that your bill contains an error and why it is wrong, and the date and amount of the error.
- Pay all other charges. You do not need to pay the disputed amounts.

Consumers should be aware that if a deal looks too good to be true, it probably is. In one scam the victim located a car on the Auto Trader website and contacted the seller directly by e-mail. He was told that the car would be shipped to him for inspection and approval if he wired the money to a bank account where it would be held in escrow. He wired the money but the car never arrived. To prevent this kind of scam consumers need to be diligent in verifying all the parties involved in the purchase by phone calls, face-to-face meetings, etc. In a similar case the consumer asked to see the car before wiring any money. The scammer ended all contacts at that point.

Another example involved a Craigslist ad for a vacation apartment rental in New York City. The renter was told he had to act fast and wire the money or he'd lose out on this good deal. All three elements of a typical scam were present in this case: (1) act fast or lose the deal, (2) wire the money, and (3) a price that was too good to be true. Scammers also use Craigslist and other websites to advertise rentals in your area. They will make a duplicate of a legitimate ad but with a much lower price and a different contact number. They will ask for cash upfront without showing the property or ask you to fill out an application with your SSN or other personal information. These are signs of the scam.

Online scams also promise great deals on airline tickets, timeshare properties, and vacation packages. The biggest red flag is when payment is requested by a wire transfer. It's difficult to track these transfers and almost impossible to get a refund. Check out the company offering the deal before making a purchase. If it and the deal appear to be legitimate, pay by credit card and not by wire. Then if the deal turns out to be fraudulent, you can dispute the charges as indicated above.

Phishing

In an e-mail scam known as "phishing" identity thieves fish for personal information by sending realistic-looking e-mail that asks recipients to go to a bogus website and provide personal information such as a credit card number, password, or Personal Identification Number (PIN). Legitimate banks and financial institutions don't send e-mails asking you to verify your account information. They already have it. The following are examples of scammers posing as the Internal Revenue Service (IRS), Federal Bureau of Investigation (FBI), Federal Deposit Insurance Corporation (FDIC), and the Centers for Disease Control and Prevention (CDC).

Each year during tax preparation time there is a surge in the number of frauds by criminals posing as IRS officials to obtain personal information for identity theft. The IRS never sends out unsolicited e-mails or asks for detailed personal and financial information. Any such e-mail is a fraud. So are telephone calls from someone stating they are from the IRS. Go to the IRS website at **www.irs.gov** for information on the latest scams and instructions on how to protect yourself from suspicious e-mails or phishing schemes. The IRS also recommends forwarding the suspicious e-mail to it at **phishing@irs.gov**.

The growing popularity of tax preparation software has led to a rise in e-mail scams targeted at do-it-yourself taxpayers. The fraudulent e-mails claim to come from a software provider and might offer a software update or download. They may ask for personal financial information or other sensitive data and contain links to websites that could download malware. Legitimate software providers routinely send customers e-mails advising them of the status of their tax returns but never ask for sensitive personal data. Any software updates should be done on your provider's website or desktop product. Also, forward any suspicious e-mails to your software provider's security center.

Fraudulent e-mails have also been sent out by criminals posing as FBI agents and officials. They give the appearance of legitimacy by using the FBI seal, letterhead, and pictures of the FBI Director. They may also claim to come from the FBI's domestic or overseas offices. Like the IRS, the FBI does not send out e-mails soliciting

personal or financial information. For more information on this kind of fraud go to the FBI website at **www.fbi.gov** and click on New E-Scams and Warnings under Be Crime Smart.

Another agency that has become aware of fraudulent e-mails in its name is the FDIC. These ask recipients to "visit the official FDIC website" by clicking on a hyperlink that directs them to a fraudulent website that includes hyperlinks that open a "personal FDIC insurance file" to check on their deposit insurance coverage. Clicking on these links will download a file that contains malicious software to collect personal and confidential information.

In 2009 the CDC issued a health alert warning people not to respond to an e-mail referencing a CDC-sponsored state vaccination program for the H1N1 (Swine Flu) contagion that requires registration on "www.cdc.gov." People that click on this embedded link risk having a malicious code installed on their computer. Examples of this and other hoaxes and rumors can be seen at **http://www.cdc.gov/hoaxes_rumors.html**.

Use the following tips to counter phishing:

- Do not open any e-mail from an unknown sender, especially if it offers something sensational, e.g., a video of Osama Bin Laden's death. Delete it without opening it. "Drive-by spam" can automatically download malware when an HTML e-mail is opened. You don't have to click on a link or open an attachment to get infected. Another way to prevent this kind of attack is to deactivate the display of HTML e-mails and display e-mails in pure-text format only.
- Do not open any unexpected e-mail attachments.
- Do not give out any passwords or personal information no matter what the e-mail says, e.g., that you will be locked out of your account if you don't provide the information.
- Do not click on links in e-mail messages purporting to come from your bank or any other institution or business that you have an account with. Retype the address into your browser. If you do click on a link and are prompted to log in with your password, don't do it. Close your browser and log into your account to make a payment or do whatever the message said.
- Do not double click on any Internet pop-up with a link to an offer or provide any personal information in response to a pop-up offer. And never enter personal information on a pop-up page.
- Use the latest versions of Internet browsers, e.g., Microsoft Internet Explorer 8, which is designed to prevent phishing attacks. Use Explorer in the "protected mode," which restricts the installation of files without the user's consent, and set the "Internet zone security" to high. That disables some of Explorer's less-secure features. And set your operating system and browser software to automatically download and install security patches.
- Make sure the website page you are entering sensitive information on is secure. You can tell it is secure when the address on the top of your screen where the Uniform Resource Locator (URL) is displayed begins with **https://** rather than **http://.** You can also look for a closed padlock or an unbroken key on the bottom of your screen to indicate the page is secure. If the lock is open the site or the key is broken, the page is not secure. Note that on many websites only the order page will be secure.
- Read the website's privacy policy. It should explain what personal information it collects, how the information is used, whether it is provided to third parties, and what security measures are used to protect the information. Consider taking your business elsewhere if you don't see, understand, or agree with the policy.
- Keep your computer up to date with the latest firewalls and anti-virus, anti-spyware, and anti-adware software. The latter are designed to protect against software that either self-installs without your knowledge or is installed by you to enable information to be gathered covertly about your Internet use, passwords, etc. This kind of software is often installed when you visit websites from links in e-mails. Use security software that updates automatically. Visit **www.OnGuardOnline.gov** for more information.
- Do not buy or download free anti-spyware software in response to unexpected pop-ups or e-mails, especially ones that claim to have scanned your computer and detected viruses.
- Make sure the pop-up blocker in the tools menu of your browser is turned on. This will prevent most pop-up ads. If you do get one, be careful in getting rid of it. Never click on any of its boxes. By clicking on No or Close you may actually be downloading malware onto your computer. And even clicking on the X in the upper right-hand corner can initiate a download instead of closing the pop-up. To be safe on a PC, hold down the Ctl and Alt keys and hit Delete. Then in the Windows Security box click on Task Manger, and then click on End Task. This will clear your screen. Then run a full computer security scan.

- Do not respond in any way to a telephone or e-mail warning that your computer has a virus even if it appears to come from an anti-virus software provider like Microsoft, Norton, or McAfee. "Helpful hackers" use this ploy to get you to download their software to fix the virus or sell you computer monitoring or security services to give them remote access to your computer so they can steal your passwords, online accounts, and other personal information. If you already have anti-virus software on your computer you'll receive a security update or warning directly on your computer.
- Look for valid trust marks to increase your confidence in using a website. Reputation trust marks like BBBOnline offer a basic level of proof that there is an actual business behind the website and that it follows proper business practices. Privacy trust marks like TRUSTe indicate that the business is aware of identity theft and personal data abuse and abides by the requirements of the trust mark provider in its privacy policy. A Secure Socket Layer (SSL) trust mark like VeriSign indicates that the site uses up-to-date encryption technology to scramble communications between the website and your computer. And security-scanning trust marks like McAfee SECURE indicate that the business uses a regularly scheduled security auditing service for its website to ensure that it is free of viruses, spyware, adware, etc. Because a phisher could create a false trust mark and verification website, you cannot know that the mark is valid unless you click on it. A link will take you to the verification website of the trust mark provider. The trust mark is valid if its verification website has **https://** in its URL.
- Be careful in visiting websites that don't have trust marks.

Spear Phishing

This is a more sophisticated version of phishing. It targets groups of people who have something in common, e.g., they work for the same company, deal with the same financial institution, or attend the same college. The fraudulent e-mails come from organizations the potential victims would normally get e-mails from. Success in spear phishing depends on three things: (1) the apparent source of the e-mail must be a known and trusted individual or organization, (2) there is information in the e-mail that makes it look legitimate, and (3) the request for personal or company-privileged information, or direction to click on an included link must have a logical basis, e.g., to update usernames and passwords. The information needed for these things is obtained hacking into the organization's computer network, data breaches, or combing through other websites, blogs, and social networking sites. Here are some things to do to avoid becoming a spear phishing victim.

- Remember that most companies, banks, agencies, etc. don't request personal information by e-mail. If in doubt, call the sender. But don't use the number in the e-mail. It's usually phony too.
- Use a browser with a phishing filter.
- Never follow a link from an e-mail to a secure website. Enter the URL manually.

Smishing

This is phishing with text messages instead of e-mails. "Smishing" is a term coined from Short Message Service (SMS) and phishing. In these scams you may receive a SMS stating that your account will be charged for some particular program or purchase unless you visit a given URL within two days to cancel the order. When you click on the cancel link you will download malware to your computer. Do not respond to these SMSs. Alternatively, the SMS may give you a phone number to call where you will be asked for personal information. Before calling verify that the number matches the number of the named institution, e.g., your bank. And never give out personal information unless you have initiated the call.

Vishing

In this scam criminals use Voice over Internet Protocol (VoIP) technology to make telephone calls from anywhere in the world pretending to be a legitimate business, often using a fraudulent called ID matching the identity of the misrepresented company. The term "vishing" comes from voice phishing. It directs recipients to call an illegitimate telephone number where they are tricked into giving up personal financial information. They might receive an urgent recorded message telling them that their credit card has been compromised and directing them to call the following telephone number immediately and punch in their 16-digit account number to verify their identity. Alternatively, you may receive an e-mail asking you to call a particular number to prevent your account from being blocked. Someone there will attempt to get you to give up personal information. The best defense

against vishing is to treat any unsolicited telephone message with suspicion and only give your personal information out when you have initiated the call and are sure the other party is legitimate.

Whaling

In another scam known as "whaling" fake e-mails have been sent to high-ranking executives to trick them into clicking on a link that takes them to a website that downloads software that secretly records keystrokes and sends data to a remote computer over the Internet. This lets the criminal capture passwords and other personal or corporate information, and gain control of the executive's computer. In one case fake subpoenas have been sent to executives commanding them to appear before a grand jury in a civil case. The link that offers a copy of the entire subpoena downloads the malicious software.

Social Networking Dangers

Malware creators, identity thieves, and spammers are increasingly targeting users of social networking sites in an effort to steal personal data and account passwords. One of the tactics they use to gain access to this information involves sending social networking users e-mails that appear to come from online friends. For example, some Facebook users have been receiving e-mails from their "friends" that claim to contain a video of them. When they click on it they download malware that installs a malicious program on their hard drive. A virus known as Koobface sends itself to all the friends on the victim's Facebook profile. A new version of the virus also is affecting users of MySpace and other social networking sites. Cyber-criminals are tricking social networking users into downloading malicious software by creating fake profiles of friends, celebrities, and others. Security experts say that such attacks, which became widespread in 2008, are increasingly successful because more and more people are becoming comfortable with putting all kinds of personal information about themselves on social networking sites. They warn that users need to be very careful about what information they post because it can be used to steal their identities. Facebook users should become a fan of its security page at **www.facebook.com/security**, which has posts related to all sorts of security issues, tips, resources, and other information.

To avoid problems on social networks or anywhere in the Internet, users should:

- Never post any information that you don't want made public. Once it's posted you cannot retract it or control its distribution.
- Never post any information that might make you or your property vulnerable, e.g., your address or travel plans.
- Wait until you get home to post your vacation blog and photos. If you do publish photos on the Internet first remove the geotags with a metadata removal tool.
- Not to click on any links, videos, programs, etc. provided in messages, even if a "friend" encourages you to click on them.
- Get program updates from the company's website, not through a provided link.
- Customize your personal privacy settings so only your friends have access to the information you post. Default settings on many sites allow anyone to see information about you. And check your settings frequently because they could be compromised when the site is updated, e.g., when new features are added.
- Read your network's privacy policy regularly to stay informed on how it uses or discloses your information. Choose to opt out of information sharing wherever possible.
- Scan your computer regularly with updated anti-virus, anti-spyware, and anti-adware programs.
- Know who your friends are and be careful about accepting and adding new ones. Be very cautious about revealing information about yourself if you chat with people you don't know.
- Be suspicious of anyone, even a "friend," who asks for money over the Internet.

Illegitimate Websites

Cybercriminals are now creating illegitimate websites that will receive high search-engine rankings and thus attract the attention of persons searching for information on a particular subject. Persons just visiting those sites risk having their computers infected with malware. And if they click on any links in those sites they risk becoming a victim of identity theft and various scams, e.g., ones that claim you can make a lot of money for a small initial investment. To avoid these problems users should:

- Keep your computer's anti-virus, anti-spyware, and anti-adware systems up to date with the latest firewalls and software.
- Use caution clicking on links that claim to provide videos or information on hot topics in the current news, e.g., the earthquakes in Haiti and Chile. And be aware that the bad guys are now tricking Google into telling you that the link is a PDF file, which makes it look more authentic.
- Do not click on links to other websites. Look up the address elsewhere and retype it into your browser.
- Check to see where you would actually go before you click on a link. You can do this by scrolling your mouse over the link and reading the address in the box that will pop up over the link. Do not click on the link if this address does not match the one in the link.
- Use the tips provided above to counter phishing.

Do the following to make sure a website is legitimate, especially if you are planning to make a purchase of a name brand product:

- Check that the domain name is spelled correctly. Cyber criminals are known to engage in type- or cyber-squatting to lure unsuspected victims to fake websites where they try to obtain personal and financial information or install malware on the victim's computer. They would use a name Appple.com or Bestbuyh.com. The fake website would be designed to look like the real one. It might offer a discount coupon in exchange for personal information or a credit card number.
- Check that the domain name ends in **.com**, **.org**, or **.net**. Those ending in **.cn** for China or **.mn** for Mongolia are likely to be fraudulent.
- Call the phone number posted and talk to a live person.

E-card Dangers

You receive an e-mail saying "A friend has sent you an e-card." The e-mail appears to be from a legitimate card company, but malware is downloaded into your computer when you click the link to see the card. You should delete the e-mail if you don't recognize the sender or if you are instructed to download an executable program to view the e–card. And make sure your computer has adequate anti-virus, anti-spyware, and anti-adware protection.

And even if you recognize the sender your computer could be harmed if the incoming e-mail is phony and you click on a link to an e-card or open an attachment. This happened around Christmas time in 2010 when employees of various government agencies received phony holiday messages that appeared to come from the White House.

Unsafe Drugs from Online Pharmacies

Buying prescription drugs on the Internet is easy but finding a safe source is not. There are thousands of Internet drug outlets selling low-price prescription medications that may be counterfeit, contaminated, or otherwise unsafe. Many of these outlets are located outside the United States, do not require a valid prescription, offer foreign drugs or ones not approved by the U.S. Food and Drug Administration, have unsecure websites, do not provide a way to contact a licensed pharmacist by phone to answer questions, and do not comply with state and federal laws and/or the patient safety and pharmacy practice standards of the National Association of Boards of Pharmacy (NABP).

You can avoid the risks of dealing with these rogue websites, which constitute about 96 percent of those on the Internet, by using safe sources have been identified by the NABP in its Verified Internet Pharmacy Practice Sites (VIPPS) program. They are listed as Recommended Internet Pharmacies on its website at **www.nabp.net**. These sites have undergone and successfully completed the NABP's accreditation process that includes a review of all policies and procedures regarding the practice of pharmacy and dispensing of medicine over the Internet as well as an on-site inspection of facilities used by the site of receive, review, and dispense medicine. The NABP website also lists Not Recommended Internet pharmacies and sites that have received its e-Advertiser Approval. These sites offer only limited pharmacy services or other prescription drug-related services. They have also been found to be safe, reliable, and lawful.

IDENTITY THEFT

Every person who willfully obtains personal identifying information, e.g., name, address, date of birth, SSN, mother's maiden name, etc. as defined in Cal. Penal Code Sec. 530.5(b), and uses that information for any unlawful purpose is guilty of a public offense. Identity theft is the fastest growing crime in the United States. Every year about 15 million people become victims. Everyone is vulnerable. Skilled identity thieves use a variety of methods to steal your personal information. These include the following:

- Dumpster diving. They rummage through trash looking for bills and other paper with your personal information on it.
- Skimming. They steal credit- or debit-card numbers with a special storage device when processing your card.
- Phishing, Spear Phishing, Smishing, Vishing, and Whaling. See preceding section on Internet Fraud.
- Changing your address. They divert your billing statements to another location by completing a change-of-address form.
- Stealing. They steal wallets, purses, mail (credit card and bank statements, pre-approved credit offers, new checks, tax information, etc.), employee personnel records, etc.

An enormous amount of information is available on various identity theft issues. Much of this is summarized in this section, which contains tips for minimizing risk, things to do if you become a victim or are notified of a security breach involving personal information, and links to many websites. For comprehensive set of links to the websites of a wide range of government agencies and nonprofit organizations that deal with these issues, go to The Consumer Federation of American's website at **idtheftinfo.org**. It contains links that deal with consumer, business, and victim resources, shopping for identity theft services, protecting yourself, statistics and studies, etc.

Some of the things you can do to minimize your risk of identity theft are listed below.

Protecting Personal Information

- Give out credit or debit card, bank account, and other personal information only when you have initiated the contact or know and trust the person you are dealing with. Beware of e-mail or telephone promotions designed to obtain personal information.
- Put strong passwords on your credit card, bank, computer, and online accounts. Avoid using easily remembered numbers or available information like mother's maiden name, date of birth, phone number, or the last four digits of your SSN. Passwords should be more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Use of non-dictionary words is also recommended. Other advice on creating strong passwords can be found at **www.microsoft.com/protect/yourself/password/checker.mspx**.
- Select password reset questions whose answers cannot be found online or from other research tools. Don't compromise a strong password with an easily answered reset question like: What is your mother's maiden name?
- Use different passwords for banking, e-commerce, e-mail, and other accounts.
- Memorize your passwords. Don't carry them in your purse or wallet.
- Keep personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your home.
- Make sure that the copying machines used by you and others who have your personal data, e.g., tax preparers, have data security measures installed to prevent unauthorized access to data on the copier's disk.
- Protect you health insurance cards like you would your credit or debit cards. If asked for your policy numbers or any other personal information in a doctor's office, make sure no one else is near enough to hear or see them.
- Protect your Medicare card number as you would your SSN. Don't give it to anyone who offers free medical equipment or services and then requests your number. And don't let anyone borrow or pay to use your Medicare card. That's foolish and illegal.
- Shred or tear up any documents with personal or financial information before throwing them in the trash. Use a cross-cut shredder.
- Avoid all online games and quizzes that request personal information, including your e-mail address. Providing this information can put your identity at risk.

Using Credit and Debit Cards

- Never loan your card to anyone.
- Pay attention to billing cycles. Check with the credit card company if you miss a bill to make sure that your address has not been changed without your knowledge.
- Only put the last four digits of your account number on checks you write to your credit card company. It knows the whole number and anyone who handles your check as it is processed won't have access to the number.
- Notify your credit card companies and financial institutions in advance of any address or phone number changes.
- Bring home all card receipts and match them against your monthly statements. Look for charges you didn't make.
- Dispose of card receipts at home. Never toss them in a public trash container.
- Call the credit card company or bank involved if a new credit card you applied for hasn't arrived in a timely manner.
- Monitor the expiration dates of your cards and contact the card issuer if new cards are not received before your card expires.
- Report all lost or stolen cards immediately and request cards with new numbers. In this case the federal Truth in Lending Act limits your liability to $50 of any charges made before you report your card lost or stolen. Contact the issuer if replacement cards are not received in a reasonable time.
- Sign and activate new cards promptly on receipt. Or write "See ID" on the signature line on the back of the card. Then a thief won't have your signature. A merchant will ask you for a picture ID to make sure you are the cardholder.
- Never put a card number on a post card or on the outside of a mailing envelope.
- Make sure only the last four digits of your card number show up on your receipts. Use of full card numbers on electronically printed receipts is prohibited by California law. (Note that the merchant copy can show the full credit card number.) Report non-complying businesses to the Methamphetamine Strike Force hotline at **(877) 662-6384**.
- Cancel accounts you don't use or need. Carry only the cards and identification you need when you go out.
- Tear into small pieces or shred any pre-approved credit card offers. They can be used by thieves to order cards in your name.
- Ask your credit card company to stop sending blank checks.
- Have your name removed from lists supplied by the Consumer Credit Reporting Companies (Equifax, Experian, and TransUnion) to be used for pre-approved/pre-screened offers of credit or insurance. Call **(888) 567-8688** or go to **www.optoutprescreen.com** to do this.
- Don't let your card out of sight. A person taking it to a Point of Sale (POS) device might have a skimmer to steal the information on the magnetic strip, copy your card number and the 3-digit security number on the back of the card, or switch cards. If you do give your card to a waiter or other sales person, make sure you get your card back. And use a credit card instead of a debit card whenever possible. With the former you don't have to pay disputed charges. But with the latter it may take the bank about two weeks to restore the funds to your account.
- Make sure your bank and credit card companies have your latest home and cell phone numbers, and e-mail address so they can contact you quickly if they suspect fraud in your accounts.
- Some credit cards now have embedded Radio Frequency Identification (RFID) chips that are designed to be read by secure card readers at distances of less than 4 inches when properly oriented for "contactless payments." Thus, RFID readers that are available to the general public and can operate at ranges up to 25 feet and are essentially useless in stealing the information on your card. And even if that information is "hi-jacked," the cards are said to have security features that make it difficult or impossible to make a fraudulent transaction. Furthermore, the information is on the chip is not the same as that on the magnetic strip, and it cannot be used to create a functioning counterfeit version of the card. If you have a card with a RFID chip and don't want to risk having the information on it stolen and used in any fraudulent activity, ask your card company for a new card without a chip.
- Beware of skimmers on self-checkout terminals at grocery stores, gasoline pumps, and other places where you might swipe your credit or debit card. Things to watch for are listed below under Using an ATM.

Protecting Your U.S. Passport

- Since August 2007 all passports issued by the U.S. State Department have a small contactless RFID computer chip embedded in the back cover. They are called "Electronic or e-passports." The chip stores the same data that is visually displayed on the photo page of the passport. It also stores a digital photograph of the holder, a unique chip identification number, and a digital signature to protect the stored data from alteration. Unauthorized reading of e-passports is prevented by the addition of a radio-frequency blocking material to their covers. The passports cannot be read until they are physically opened. Then there are protocols for setting up a secure communication channel and a pair of secret cryptographic keys in the chip to ensure that only authorized RFID readers can read the data on the chip.
- In July 2008 the U.S. State Department began issuing U.S. passport cards that can be used to enter the United States from Canada, Mexico, the Caribbean, and Bermuda at land border crossings or seaports of entry that are less expensive that a passport book. It cannot be used for international travel by air. To increase speed, efficiency, and security at U.S. land and sea border crossings the card contains a RFID chip. However, no personal information is on the chip. It only points to a record stored at secure U.S. government databases. And a protective RFID-blocking sleeve is provided with each card to prevent unauthorized reading or tracking of the card when it is not in use. Make sure you carry the card in the sleeve.

Protecting Your SSN

- Examine your Social Security Personal Earnings and Benefits Estimate Statement for possible fraud. You will receive it about three months before your birthday each year.
- Provide your SSN only when it is required by a government agency, employer, or financial institution. In a recent case a man received a call from a person who claimed to be a jury coordinator and said that a warrant has been issued for his arrest because he failed to report for jury duty. When he protested that he never received a summons he was asked for his SSN and date of birth to verify the records. Caught off guard he provided this information. Instead he should have hung up realizing that court workers would never ask for a SSN or other personal information.
- In a variation of the above scam, the caller says that you've been selected for jury duty and asks you to verify your name and SSN. Remember, notification of jury duty is always done by mail.
- Never use your SSN for identification. Don't carry it or your Social Security card in your purse or wallet.
- Do not have your SSN or driver's license number printed on your checks. And never write your SSN on a check.
- Provide your driver's license or some other identification number when reporting a crime in which you are the victim. Do not provide your SSN. The crime report will be available to the defense if a suspect is prosecuted.

Managing Your Accounts

- Keep a record in a secure place of all your credit and debit card, and bank and investment account phone numbers for quick reference if identity theft occurs.
- Review your bank statements carefully. Match your checkbook entries against paid checks. Look for checks you didn't write.
- Never leave transaction receipts at bank machines or counters, trashcans, gasoline pumps, etc.

Carrying Personal Information in a Purse or Wallet

- Carry only a driver's license, cash, and one credit card. Don't carry blank checks or a checkbook. Don't carry anything with a PIN written on it.
- Keep a record of its contents. Photocopy both sides of your credit and debit cards and driver's license and keep them in a safe place at home.
- Don't carry your Social Security card or anything with your SSN on it. Persons with Medicare cards should carry photocopies of the cards with the last four digits of their SSN removed. Keep the card is a safe place at home.
- If you carry a wallet in a purse, keep credit or debit cards in separate compartment and not in your wallet.
- Don't carry personal information of your family members.

- Don't carry any account or computer passwords.
- Take the measures listed below for victims of identity theft if your wallet is lost or stolen. Don't wait for someone to find and return it. These include filing a police report, reporting your credit and debit cards missing, closing checking accounts, having a fraud alert placed on your credit reports, notifying your medical insurance companies, reporting a missing driver's license, etc.

Using the Mail

- Deposit outgoing mail at a Post Office, in a blue U.S. Postal Service collection box, or give it directly to your mail delivery person. Put it in a collection box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Also, do not leave mail for pickups from personal curbside boxes or cluster box units.
- Pick up your mail as soon as possible after it arrives in your personal curbside box or cluster box unit. If this is not possible, have a trusted friend or neighbor collect your mail, especially if you are expecting a box of checks or a new credit or debit card.
- Consider having new checks mailed to your bank for collection to avoid possible theft from your mailbox.
- Use a locked mailbox and make sure the lock works.
- Investigate immediately if bills do not arrive when expected, you receive unexpected credit cards or account statements, you are denied credit for no apparent reason, and you receive call or letters about purchases you did not make.
- Report the non-receipt of expected valuable mail by calling the sender and the Postal Inspection Service as soon as possible.

Using an ATM

- Use ATMs that are inside a store or a bank. These are less likely to have been tampered with for skimming, which is the illegal capture and utilization of a cardholder's financial information from an ATM transaction. If you use an outside ATM, it should be well-lighted and under video surveillance.
- Get off your cell phone and be alert when using an ATM.
- Check the machine and everything around it before you take out your card. Look for parts that seem crooked or have a different color, or decals that are partially covered. If something doesn't seem right, go to another machine.
- Most ATMs have flashing lights in the card slot. Their obscuration is a sign of tampering.
- Look to see if there is anything in the slot where you insert your ATM card. Thieves place a small, hard-to-detect skimming device in the card slot to steal your PIN and other bank account information. If anything looks suspicious, give it a pull or push. Skimmers are usually held in place loosely by glue or tape to make them easy for the thief to remove. If you remove one, contact the SDPD immediately. Don't throw it away or keep it; that would make it look like you are running the scheme.
- Check for a false keypad that has been installed over the built-in one. False keypads stick out too far or look strange.
- Check the area around the machine for hidden cameras. To be safe shield your hand when entering your PIN so it can't be seen by anyone near you or by a hidden camera.
- If you use a debit card memorize your PIN and keep it secret. Don't write it down or keep it in your wallet or purse.
- Keep the customer-service phone numbers of your bank and credit-card company readily available. Call the appropriate number immediately if your card gets stuck in an ATM. Do not leave the ATM.
- Don't leave your transaction receipts at the ATM. Take them home and use them in balancing your account.
- Monitor your bank statements frequently and report any unauthorized activity immediately.

Buying Identity Theft Protection

- You cannot buy absolute protection against identity theft. Beware of any such claims, especially regarding prevention of misuse of existing credit-card accounts, theft of medical records, and theft of personal information from employer's personnel files.
- Before signing up for protection, be sure to understand what services are provided, what protections they afford, and how the personal information you provide is protected.

- Fraud alerts, which provide some protection against new-account fraud, do not provide absolute protection and only deal with a small fraction of identity theft incidents.

Checking for Possible Identity Theft

- Obtain free copies of your credit reports from the three nationwide consumer credit reporting bureaus (Equifax, Experian, and TransUnion) by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**. This is the ONLY source of free reports authorized under Federal law. You can get one free report annually from each bureau. Stagger your requests to obtain one every four months. That way you can monitor your credit during the year. Check these reports for errors, fraudulent activities, e.g., accounts opened without your knowledge or consent, and persons or businesses checking on your credit. Contact the reporting bureau immediately if you see any inaccuracies. These bureaus may also try to sell you credit monitoring products or services for a fee. The FTC requires that any advertising for such products or services be delayed until after you get your free credit reports.
- Be aware that if you order a free credit report from an unauthorized website such as **freecreditreport.com** you will be given a free limited-time trial membership in its credit monitoring service that will provide daily monitoring of your credit reports, alert notices of key changes, bi-monthly credit scores, etc. If you don't cancel this membership you will be charged a fee for each month that you remain a member. Before becoming a member you need to understand exactly what protection and services it will and will not provide, and whether you need the additional protection. Some services you will pay for you can do yourself at no cost, e.g., ordering credit reports and placing fraud alerts.
- These websites are required to print a disclosure that states the following at the top of each page that mentions free credit reports: "THIS NOTICE IS REQUIRED BY LAW. Read more at **www.FTC.gov**. You have the right to a free credit report from **www.AnnualCreditReport.com** or **(877) 322-8228**, the ONLY authorized source under federal law." They are also required to include a clickable button to "Take me to the authorized source" and clickable links to **www.AnnualCreditReport.com** and **www.FTC.gov**. However, neither of these requirements is enforced by the FTC so they don't appear on websites that advertise free credit reports.
- Place a security freeze on your credit reports. This will protect you against fraud in new accounts by prohibiting the credit reporting bureaus from releasing your credit reports to a potential creditor without your express permission. Go to their websites for the procedures and fees for placing and lifting freezes. Their addresses are: **www.equifax.com**, **www.experian.com**, and **www.transunion.com**.
- Check your medical bills and health insurance statements to make sure the dates and types of services match your records. Read every letter you get from your insurer, including those that say "this is not a bill." If you see a doctor's name or date of service that isn't familiar, call the doctor and your insurer.
- Once a year request a list of all benefits paid in your name by your health insurer. If the thief has changed your billing address you would not be receiving any bills or statements.

Protecting Your Child's Identity

- Provide your child's SSN only when it is required by a government agency or financial institution. Never provide it for identification.
- Carry your child's SSN or card in your purse or wallet only when you know you will need it.
- Teach your child never to give out personal information over the phone or on the Internet.
- Check to see if your child has a credit report. There should not be one unless someone has applied for credit using your child's SSN number. No minor should have a credit report. At a FTC-sponsored forum on child-centric fraud in July 2011 it was estimated that more than 140,000 American children become victims of identity theft each year. By various means thieves obtain children's SSNs and sell these genuine numbers to persons with poor credit ratings who obtain credit cards, make extensive purchases, and don't pay their bills. If this happens you should contact the credit card companies and the three nationwide consumer credit reporting bureaus immediately.
- Watch your child's mail for credit card applications, bills, or bank statements. They are signs that someone has started a credit history in your child's name.
- Request that banks in which your child has an account remove his or her name from marketing lists.
- Report any suspected identity theft to the three nationwide consumer credit reporting bureaus and obtain copies of any credit reports in your child's name and SSN. If your child does have a credit report, ask to have all

accounts, application inquiries, and collection notices removed immediately. Tell the credit issuer that the account is in the name of your minor child who by law isn't permitted to enter into contracts.

- Take advantage of your rights under the federal Children's Online Privacy Protection Act (COPPA). This law requires websites to get parental consent before collecting and sharing information from children under 13. COPPA covers sites designed for children under 13 and general audience sites that know certain users are under 13. It protects information that websites collect upfront and information that children give out or post later. It also requires these sites to post a privacy policy that provides details about the kind of information they will collect and what they might do with the information. You should: (1) know your rights, (2) be careful with your permission, (3) check out the sites your children visit, (4) review the sites' privacy policies, (5) contact the site if you have any questions about its privacy policy, and report any site that breaks the rules to the FTC at **www.ftc.gov/complaint**. For answers to frequently asked questions about the Children's Online Privacy Protection Rule go to **http://www.ftc.gov/privacy/coppafaqs.shtm**.

If You Become a Victim

File a police report as soon as possible if you become or may become a victim of identity theft. Call the SDPD non-emergency number, **(619) 531-2000** or **(858) 484-3154**. Then do the following:

- Set up a folder where you can keep a log of all your reports and supporting documents, and contacts and their phone numbers.
- Contact the FTC to report the theft. Its Identity Theft Hotline is **(877) 438-4338**. Or visit its website at **www.ftc.gov/idtheft**. The FTC is the federal clearinghouse of complaints of victims of identity theft. It helps victims by providing information to resolve financial and other problems that could result from identity theft. Its booklet entitled *Take Charge: Fighting Back against Identity Theft* deals with bank accounts and fraudulent withdrawals, bankruptcy fraud, investment fraud, phone fraud, and other specific problems. It also describes the immediate steps victims should take and ways to minimize recurrences.
- Report the theft to the fraud units of Equifax at **(800) 525-6285**, Experian at **(888) 397-3742**, and TransUnion at **(800) 680-7289**. Ask to have a fraud alert placed on your credit reports. It will tell creditors to follow certain procedures before they open new accounts in your name or make changes to you existing accounts. In placing a fraud alert you will be entitled to free copies of your credit reports. Review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Fraud alerts are good for 90 days and can be renewed. They are free.
- Alert your banks of any fraud and request new account numbers with new checks, ATM cards, and PINs. Also provide new passwords and stop payment on any missing checks.
- Contact all your creditors by phone and in writing to inform them of the fraud.
- Call your credit card companies and request account number changes. Don't ask to cancel or close your accounts; that can hurt your credit score, especially if you have outstanding balances. Say you want a new numbers issued so your old numbers will not show up as being "cancelled by consumer" on your credit reports. Also change your PINs and passwords.
- Call the security or fraud departments of each company you have a charge account with to close any accounts that have been tampered with or established fraudulently. Follow up the request in writing and ask for written verification that the accounts have been closed and any fraudulent debts discharged. Keep copies of all documents and records of all conversations about the theft. If you still want a charge account, request a new number.
- Report the loss of your SSN to the IRS. This will alert the IRS that someone might use your SSN to get a job or file a tax return to receive a refund. Call its Identity Theft Hotline at **(800) 908-4490** and go to **http://www.irs.gov/privacy/article/0,,id=186436,00.html**. Follow the directions there regarding identity theft and your tax records, and the need to provide it with proof of your identity. And read "Ten Things the IRS Wants You to Know about Identity Theft" on its main website at **www.irs.gov**. Also contact the Social Security Administration (SSA) on its Fraud Hotline at **(800) 269-0271** or by e-mail to the Office of the Inspector General at **www.ssa.gov/org**.
- Call the U.S. Secret Service at **(619) 557-5640** if the crime involves counterfeit credit cards or computer hacking.
- Contact the California DMV Fraud Hotline at **(866) 658-5758** to report the theft and see if another driver's license has been issued in your name.

- Notify the U.S. Postal Inspector if your mail has been stolen or tampered with. Its number is **(626) 405-1200**. Or report it online at **http://postalinspector.uspis.gov**.
- In the case of medical identity theft request a copy of your current medical files from each health care provider, and request that all false information be removed from your medical and insurance files. Enclose a copy of the police report with your requests. For more information things to do if you are a victim of medical identity theft or concerned about it go the World Privacy Forum's website at **www.worldprivacyforum.org/ medicalidentitytheft.html**.
- Call the Health Insurance Counseling and Advocacy Program's Senior Medicare Patrol (HICAP/SMP) at **(800) 434-0222** to report any fraud involving Medicare.
- If you are contacted by a collector for a debt that resulted from identity theft, send the debt collector a letter by certified mail, return receipt requested, stating that you did not create the debt and are not responsible for it. Include a copy of the police report you filed for the identity theft crime and a completed copy of the FTC's Identity Theft Victim's Complaint and Affidavit. It can be downloaded from its website at **www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf**. Also write in your letter that you are giving notice to a claimant under California Civil Code Sec. 1798.93(c)(5) that a situation of identity theft exists.
- Other things you should do as a victim are in the Identity Theft Victim Checklist on the website of the California Office of Privacy Protection at **www.privacy.ca.gov/cis3english.htm**. It's website at **www.privacy.ca.gov** contains additional tips on avoiding and resolving identity theft problems.

Another useful website is that of the Identity Theft Resource Center (ITRC) at **www.idtheftcenter.org**. It contains information ranging from advice for people who have had a wallet stolen to tips for reducing the risks of identity theft. It also contains fact sheets, solutions to various identity theft problems, letter forms, scam alerts, a "Help, I'm a Victim of Identity Theft" button, and answers to frequently asked questions. Its toll-free victim-assistance number is **(888) 400-5530**.

If You Are Notified of a Security Breach Involving Personal Information

Most states now have security breach notification laws under which a person whose personal information is compromised must be notified of the breach. The California Breach Notification Law is in Civil Code Sections 1798.29, 1798.82, and 1798.84. The first applies to state government agencies; the other two apply to any person or business doing business in the state. The notice requirement is triggered if the breach involves a person's name in combination with any of the following: SSN; driver's license or California Identification Card number; financial account, credit card, or debit-card number along with any PIN or other access code required to access the account; medical information; or health insurance information. You should do the following for each and also be alert for possible spear phishing as defined above under Internet fraud and other crimes:

- SSN. Put a fraud alert on your credit reports at Equifax, Experian, and TransUnion, and order copies of your reports. Review them carefully and file a police report if you find anything suspicious. If you don't find anything suspicious at first, renew the fraud alert and check your credit reports periodically. Also report the loss to the IRS and SSA.
- Driver's License or California Identification Card number. Call the DMV Fraud Hotline to report the incident.
- Financial account numbers. Call the institution to request new account numbers and PINs. And put new passwords on your accounts.
- Medical or health insurance information. Review your explanation of benefits statements and contact your insurer if you see any services you did not receive.

For additional information on this and other privacy issues visit the Privacy Rights Clearinghouse's website at **www.privacyrights.org**.

WI-FI HACKING AND HOTSPOT DANGERS

Use of Wi-Fi in coffee shops, libraries, airports, hotels, universities, and other public places pose major security risks. While convenient, they're often not secure. You're sharing the network with strangers, and some of them may be interested in your personal information. If the hotspot doesn't require a password, it's not secure. If it asks for a password through your browser simply to grant access, or it asks for a Wired Equivalent Privacy (WEP) password, it's best to treat it as unsecured. You can be more confident that a hotspot is secure only if it asks for the

Wi-Fi Protected Access (WPA and WPA2) password. WPA2 is more secure. However, a flaw in a feature added to Wi-Fi called Wi-Fi Protected Setup (WPS) allows WPA and WPA2 security to be bypassed and broken by brute force in many situations.

Also, unsecure laptops and smart phones make it easy for a hacker to intercept information to and from the web, including passwords and credit- or debit-card numbers. They are also vulnerable to virus and spyware infections, and to having their contents stolen or destroyed. A hacked laptop or smart phone can also create a security risk for the user's workplace if it contains a password to the corporate network. Wi-Fi users should take the following steps to reduce these risks:

- Turn the Wi-Fi on your laptop, PDA, and smart phone off when you aren't using the network. Otherwise your Wi-Fi card will broadcast your Service Set Identifier (SSID) looking for all networks it was previously connected to. This enables hackers to figure out the key that unscrambles the network password.
- Use a known service instead of Free Public Wi-Fi or similar risky, unknown signals called ad hoc networks.
- Check the Wi-Fi security policies of your service provider and install the protections they offer to ensure it's a known network and not an "evil twin" hacker site pretending to be the legitimate one.
- Pay attention to warnings that a Secure Sockets Layer (SSL) certificate is not valid. Never accept an invalid certificate on a public wireless network. Log off and look for a trustworthy network. Look for the padlock indicating an SSL connection. Keep your firewall on. And keep your operating system updated.
- Find out if your company offers a Virtual Private Network (VPN) and learn how to use it. Encrypted VPN sessions offer the highest security for public wireless use. Use Hypertext Transfer Protocol Secure (HTTPS) when accessing a website or use a VPN to protect the transmission of sensitive information when using a wireless connection.
- Upgrade your Wi-Fi cards. The older WEP security is easily hacked. The new WPA and WPA2 are much more resistant to attack.
- Secure IEEE 802.11 wireless access points with a WPA2 and Advanced Encryption Standard (AES) encryption to protect sensitive communications.
- If your router has the WPS function, disable it. Methods have been published for doing this for some models. But on others, disabling the WPS in the user interface is not effective and the device remains vulnerable to attack.
- Learn to connect securely. Even the vulnerable WEP offers more privacy and protection than an unsecured public connection. It's not something the average hacker can crack. Make sure your connection is legitimate. Look at your connection page for a name and description. A legitimate wireless network is simply called a "wireless network." It will display an icon of just one connected computer. So called ad hoc or peer-to-peer networks that are used by scammers to steal your personal information scammers are not legitimate. The will be called "computer-to-computer" networks and display an icon of several computers connected together. Never connect to this network. And be sure to set up your computer so it doesn't automatically connect to a network but allows you to choose a connection.
- Only log in or send personal information on website pages that are encrypted. They will have **https://** or **shttp://** in their URLs and a "lock icon" at the top or bottom of your browser window. You can click on this icon to display information about the website and help you verify that it's not fraudulent.
- Use a different password for each account.
- When you've finished using an account, log out. Don't stay signed in.
- Pay attention to warnings from your browser if you try to visit a fraudulent website or download a malicious program.
- Remove all passwords and browsing history after using a shared computer.
- Disable file-sharing on your laptop.
- Don't send any sensitive personal or business information while in a hotspot unless you absolutely have to.
- Put strong passwords on your wireless network. Passwords should be more than eight characters in length and have at least one capital letter, one lowercase letter, one number, and one symbol. Other advice on creating strong passwords can be found at **www.microsoft.com/protect/yourself/password/checker.mspx**.
- In shopping, it's fine to browse website when you're out but wait until you are at home to do any online business.
- Be aware of the existence of malware that enables a mobile phone to be used as an open microphone with or without the owner's knowledge.

And corporate Information Technology (IT) managers should do the following to protect corporate data from hotspot dangers:

- Establish and enforce strong authentication policies for devices trying to access corporate networks
- Require employees to use a corporate VPN and encryption when making connections and exchanging data. Better still, set up computers so that devices automatically connect to the VPN and encrypt data after making sure that the computer or device hasn't been lost or stolen.
- Make sure all devices and software applications are configured properly and have the latest patches.
- Ensure that corporate security policies prevent employees from transferring sensitive data to mobile devices or unauthorized computers.
- Provide employees with broadcast air cards that require a service plan so they don't have to use public hotspots for wireless connections.
- Be aware of the existence of malware that enables a mobile phone to be used as an open microphone with or without the owner's knowledge.

OTHER SCAMS

This section contains tips on recognizing and avoiding scams involving additional veterans benefits, appeals for help, auto load modification, bankruptcy foreclosure rescue, cash-back, charities, checks from unknown parties, check washing, credit repair, debt settlement, dishonest tax return preparers, earned income tax credit, empty box bargains, fraudulent checks, free samples, gift card stripping, Green Dot MoneyPaks, green energy conservation, healthcare fraud, high-pressure sales of financial products at free-meal seminars, immigration services, investment opportunities, job offers, landlord impersonation, Medicare enrollment, post-foreclosure solicitations, predatory insurance sales practices, prize notification and lotteries, property tax relief, reverse mortgages, short sales of homes, tax debt relief, third-party telephone bill charges, timeshare transactions, and unscrupulous contractors.

Information on preventing these and many other scams is available at no cost from the California Department of Consumer Affairs. A complete list of its publications is online at **www.dca.ca.gov/publications/index**. Publications can be viewed online or ordered by calling **(866) 320-8652**. Additional information about protecting yourself from fraud and identity theft is available on **www.STOPFRAUD.gov**, the website of the Federal Financial Fraud Enforcement Task Force established in 2009 to improve federal and state government efforts to investigate and prosecute significant financial crimes, and to recover their victim's losses.

Also, any San Diego resident over the age of 60 can obtain free legal advice on recouping money lost to scams by calling Elder Law & Advocacy at **(858) 565-1392**. This state- and county-funded nonprofit corporation provides no-cost routine legal services to seniors and caregivers of seniors.

Additional Veterans Benefits

In this scam unscrupulous investment sales agents promise older veterans that they can get them additional benefits by overhauling their investments. This usually involves the transfer of a veteran's retirement assets to an irrevocable trust to make the family appear impoverished so the veteran can qualify for a pension and related programs that pay additional benefits for everyday living expenses. The investments are either completely bogus, in which case the veteran loses all his or her assets, inappropriate for older retirees, or ones that generate a high commission for the agent. While the Veterans Administration does not examine veterans' asset histories for determining pension eligibility, Medicaid does and its benefits can be jeopardized by such asset transfers. Veterans can avoid this scam by doing the following:

- Don't be fooled by agents who say they represent official-sounding veterans' organizations.
- Be wary of sales pitches made at free-meal seminars sponsored by nursing homes, community centers, assisted-living facilities, etc. They often receive a fee to let sales people make so-called educational presentations. (See the section on high-pressure sales of financial products at free-meal seminars above.)
- Contact the California Department of Veterans Affairs at **(800) 952-5626** for official information about veterans benefits. Or see an overview of the benefits administered by the Department at **http://www.cdva.ca.gov/VetService/Overview.aspx**.

- Contact the Financial Services Division of the California Department of Corporations at **(866) 275-2677** to find out if the sales agent is licensed. Or get license information directly at **http://www.dre.ca.gov/gen_lic_info.html**.

Veterans should also avoid dealing with companies that offer cash in exchange for an assignment of future benefit and pension payments. While these pension buyouts and quick-cash loans are not necessarily illegal, the U.S. Department of Veterans Affairs calls these offers "financial scams" that take advantage of desperate veterans who may be down on their luck and need quick cash. The buyouts typically pay only a fraction of a veteran's actual entitlement over time, about 30 to 40 cents on the dollar. And on loans, interest rates may exceed 30 percent.

Appeals for Help

This scam usually involves a call for help from a person claiming to be a family member, e.g., a grandson, who says he's been arrested or hospitalized in a foreign country and needs cash quickly in the form of a money-wire transfer but is afraid to call his parents. Grandparents are often targeted. Scammers get the names of family members from obituaries or social networking sites on the Internet. They also use these sites to learn about foreign travel by family members. You can protect yourself by doing the following:

- Listen to the caller and take notes, including the person's called ID.
- If a caller says he's your grandson, ask which one. But don't provide a name. Most scammers will hang up.
- Ask a question that only your grandson would be able to answer correctly.
- Confirm your grandson's location and identity by saying you will return his call at his home or on his cell phone, but don't ask for the numbers. Get them from a trusted family member.
- If the call involves an arrest, contact the U.S. Embassy in the country involved and ask for assistance and verification of the arrest.
- Never provide bank account, credit-card, or debit-card numbers to any caller.
- Be very suspicious of any requests for money wires.
- Report the scam to the SDPD or the FBI. Scams coming from Canada can be reported on **www.antifraudcentre.ca**.

A variant of this is called the Red Cross scam. It preys on the family of military personnel deployed overseas. The scammer claims to be with the Red Cross and says that their loved one has been injured. They then ask for your SSN to authorize help. They might also ask for money up front. Family members should clear any injury report through the appropriate chain of command or contact the base family community services for help. They should never give out any personal information or send money.

Auto Loan Modification

If you're having trouble paying your car loan and you're worried about having your vehicle repossessed, you may think about doing business with a company that claims it can reduce your monthly car loan or lease payment and help you avoid repossession. These companies might charge fees of several hundred dollars up front, tout their relationships with lenders, and bolster their claims to be able to significantly lower your monthly payments with glowing testimonials from "satisfied" customers. Some say that if they can't make a deal with your lender, they'll refund your money.

These promises sound like a way to solve your problem. But the FTC says they're just smooth talk by scam artists who are out to take your money and provide nothing in return. Many never even contact the lenders. The scam artists often compounded the problem by telling their clients to stop making their car payments while the companies claimed to be in negotiations with lenders. Some victims learned that nothing had been done anything only after their lender contacted them about repossessing their vehicle.

If you are having trouble making car payments contact your lender directly to discuss your options as early as you can. The longer you wait to call, the fewer options you will have. Typical auto loan modifications involve either deferring missed payments to the end of the loan or extending the loan term to reduce monthly payments. That choice actually increases the total amount you pay in interest, even with a lower interest rate. Lenders rarely reduce the amount of the principal or the interest rate in an auto loan modification.

Bankruptcy Foreclosure Rescue

Bankruptcy foreclosure scams target people whose home mortgages are in trouble. Scam operators advertise over the Internet and in local publications, distribute flyers, or contact people whose homes are listed in foreclosure notices. They may promise to take care of your problems with your mortgage lender or to obtain refinancing for you. Sometimes they ask you to stop making your mortgage payments or make the payments to them. But instead of contacting your lender or refinancing your loan they pocket the money you paid and then file a bankruptcy case in your name, often without your knowledge. If this happens you could also lose your home. So proceed with care in dealing with an individual or company that:

- Makes an unsolicited contact and uses high-pressure sales techniques,
- Calls itself a mortgage consultant, foreclosure service, or similar name,
- Contacts people whose homes are listed for foreclosure,
- Promises to find "loopholes" in your load documents or violations of State or Federal lending laws that can get you off the hook,
- Asks for a fee before performing a service,
- Asks you to make your home mortgage payments directly to them, or
- Asks you transfer you property deed or title to them.

Some ways to avoid becoming a victim of a loan-modification scam are listed below:

- Do not transfer ownership of your home to someone who promises to save it.
- Do not pay advance loan-modification fees to anyone, including a real estate licensee or an attorney. Advance fees are now prohibited in California.
- Be careful in selecting an attorney. Do not rely on ads that claim the attorney is a member of the State Bar of California. All attorneys are members of the Bar and not all have special knowledge, experience, or expertise in loan modifications. In fact, it appears that many attorneys offering these services have little or no prior experience in loan modifications.
- Read all documents carefully before signing them.
- Do not make your mortgage payments to anyone other than your lender.
- Do not work with anyone who tells you not to contact your attorney, lender, or a credit or housing counselor.
- If you deal with a foreclosure consultant as defined in California Civil Code Sec. 2945.1 who is not an attorney or a real estate broker, make sure that person has obtained a Certificate of Registration as a Mortgage Foreclosure Consultant from the California Department of Justice. This is now required in California.
- Before hiring a consultant check the California Attorney General's website at **www.ag.ca.gov/loanmod** for tips to avoid being scammed and other information.

If you can't pay your mortgage, call your lender as soon as possible for help. You don't have to be in default to obtain a mortgage modification, as discussed below. The further behind you fall the more likely you are to lose your home. There are also many non-profit agencies that can help you with loan modification without a fee. You can get a list of housing counseling agencies approved by the U.S. Department of Housing and Urban Development (HUD) by state and city on its website on the page entitled Foreclosure Avoidance Counseling at **www.hud.gov/offices/hsg/sfh/hcc/fc/**. As of April 10, 2012 there were 10 HUD-approved agencies in San Diego. Their counseling services are provided free of charge. One in San Diego is Community Housing Works. It can be contacted at (619) 282-6647. Its website is **www.chworks.org**. Another is Housing Opportunities Collaborative. Its phone number is **(619) 283-2200**. Its website is **www.housingcollaborative.org**. There is no need to pay a private company for these services. Remember, if you do engage a real estate broker or attorney only pay their fee after they have completed their work.

If you suspect a scam call the Real Estate Fraud Subdivision of the San Diego County District Attorney's Office at **(619) 531-3552**. If bankruptcy proceedings are involved, call the United States Trustee at **(619) 557-5013**. The Trustee is a U.S. Justice Department official who monitors the bankruptcy system.

If you paid a licensed attorney for assistance in obtaining foreclosure relief and the attorney failed to perform legal services with competence, you should file a complaint with the State Bar by calling the Attorney Complaint Hotline

at **(800) 843-9053** or by filing a written complaint. Information on filing a complaint and the complaint form are available on the State Bar website at **www.calbar.ca.gov**. The grounds for ethics violations in dealing with foreclosures can be found on the State Bar website by searching Ethics Alert and selecting the document entitled *Legal Services to Distressed Homeowners and ...* Note that attorneys are prohibited from contacting you in person or by telephone based on a referral from a foreclosure consultant or someone else unless the attorney has a family or prior professional relationship with you.

In addition to these California remedies, consumers can file a complaint with the FTC by calling **(877) 382-4357** or going to **https://www.ftccomplaintassistant.gov/**. In its Mortgage Assistance Relief Services (MARS) Rule, the FTC is now banning mortgage relief companies from collecting advance fees and telling consumers to stop communicating with their lenders or loan servicers. It is also requiring companies to disclose the following:

- They are not associated with the government, and their services have not been approved by the government or the consumer's lender or servicer.
- The amount of their fee.
- The lender may not agree to change the consumer's loan.
- Consumers may lose their home and damage their credit rating if they stop paying their mortgage.
- Consumers may stop doing business with the company at any time, accept or reject any offer the company obtains from the lender or servicer, and if they reject the offer, they don't have to pay the company's fee.

Companies are also prohibited from making any false or misleading claims about their services or those of any alternative relief providers, the likelihood of consumers getting the results they seek, or the amount of money consumers will save by using their services.

Under the federal Making Home Affordable Program borrowers can apply for a mortgage modification if they are having difficulty paying their mortgage because their payment has increased significantly, their income has declined, or they have suffered a hardship, e.g., unexpected medical bills. There is no requirement for default. The following other requirements apply:

- The amount owed on the first mortgage must be equal to or less than $729,750.
- The mortgage must be older that Jan. 1, 2009.
- The current monthly payment is more than 31 percent of your gross monthly income
- You must be able to pay up to 31 percent of your gross monthly income on a reasonable mortgage

Cash-Back Scams

This scam involves credit or debit card transactions with dishonest cashiers at retailers. In it the cashier would also ring up a "cash-back" charge and pocket the cash amount. To prevent this scam make sure the transaction total on your receipt and the register matches the amount or your purchases if you did not request any cash back. And report any differences to the store manager.

Charity Scams

Scammers often pose as charities and solicit donations for emotional causes such as children with life-threatening disease, wounded veterans, police and firefighters, etc. In many instances they use a name similar to a legitimate charity to mislead donors, e.g., "American Cancer Research Society" instead of the American Cancer Society. They are also more aggressive than legitimate charities, often calling you at home or coming to your door. Keep in mind that legitimate charities, in contrast to scams, will not pressure you to donate on the spot. The following tips will help protect you from these scams.

- Check out any suspicious "charities" on the California Attorney General's or BBB's websites at **www.ag.ca.gov/charities** or **www.bbb.org/us/charity**, respectively. Both have searchable databases that provide information on legitimate charities.
- You can also go to **www.CharityNavigator.org** for the following information on specific charities: fund-raising efficiency rate, program/administrative spending ratios, revenue/expense statements, salaries of top

administrators, and an overall rating. Most reputable charities will spend about 75 percent of their funds on their programs. Another source of information is **www.GuideStar.org**.

- Check the charity's IRS Form 990. By law non-profit organizations must make these tax forms available to the public for the last three years. They touch on everything from management policy and executive pay to conflicts of interest. And they will tell you whether the charity is financially secure. These forms can also be seen on **www.GuideStar.org.** Also check that the charity is registered as a nonprofit with the IRS. You can do this at **www.irs.gov/app/pub-78**.
- Never donate over the phone. Even if the charity is legitimate, most of the money will go to the telemarketing company that is being paid to make the calls. If you want to contribute, do so directly to the charity, not to the solicitor.
- Beware of charities that spring up over night in connection with current events or natural disasters. They may make a compelling case for your money, but as a practical matter, they usually don't have the ability to get donations to the affected areas or people.
- Beware of charities that don't have a website.
- Ask for written information about the charity's mission, how your donation will be used, and proof that your donation is tax deductible. A legitimate charity will send this to you.
- Do not respond to any solicitations by e-mail. Many are fraudulent and contain malware. If you are thinking about giving online, look for indicators that the site is secure. These are lock icons on the browser's status bar or a URL that begins with "**https**."
- Donate by check or credit card, never with cash. Write checks payable to the organization, not to a solicitor. Provide you credit card number only after you have reviewed information about the charity and verified its credibility. And ask the organization not to store your credit card information.
- Keep a record of your pledges and contributions. Callers may try to trick you by thanking you for a pledge you didn't make. If you don't have a record of a pledge or contribution, resist the pressure to give.
- Remember that "free" goods offered as an incentive in raising funds are paid for out of your contribution, which means less money is available to the charity.

You may need to dig deeper in vetting small local charities. These can be very efficient in dealing with local problems. Here are some guidelines to follow.

- Examine the charity's mission statement. It should clearly state what the charity is trying to accomplish and how it works to achieve its goals. It is typically found on the charity's website. Ask for a copy if the charity doesn't have one. And being local, you can talk to the staff and find out how its funds are being used.
- Find out who's in charge. A small charity should have at least three board members to start. This will ensure that different ideas are being considered. Eventually it should have at least six board members to provide expertise in legal, financial, and other matters.
- Check its finances. Ask to see copies of its IRS Form 990, Letter of Determination from the IRS showing its tax-exempt status, audited financial statements, and annual reports.
- Ask about its conflict-of-interest policy regarding staff compensation and outside financial interests.
- Beware of any charity that is unwilling to answer your questions.

Checks from Unknown Parties

In one case a consumer found a $9 check with a product he had ordered. He cashed the check and later found a $149 charge on his credit card. He failed to read the small print on the back of the check which authorized the transfer of his personal information to another company that would enroll him as a member of an organization for a monthly fee. To avoid such scams never cash checks from unknown parties.

Check Washing

People who steal mail are usually looking for envelopes containing personal checks that are made out to pay bills. They wash the check with chemicals to remove the payee's name and amount. The result is a blank check signed by you. They can then fill in their names and an amount and cash it. You can prevent your checks from being stolen by depositing your mail in boxes or slots inside a post office. Or use an outside box only if there is another pickup that day. It is not safe to leave mail in a box overnight. Never leave mail for pickups from personal curbside boxes or cluster box units. And when making out checks use a pen with ink that is resistant to washing.

Credit Repair

The 1996 Credit Repair Organizations Act prohibits a variety of false and misleading statements, as well as fraud by credit repair organizations (CROs). CROs may not receive payment before any promised service is "fully performed." Services must be under written contract, which must include a detailed description of the services and contract performance time. CROs must provide the consumer with a separate written disclosure statement describing the consumer's rights before entering into the contract. And consumers can sue to recover the greater of the amount paid or actual damages, punitive damages, costs, and attorney's fees for violations of the Act.

If you encounter a CRO that promises to remove negative items from your credit reports it is safe to assume it's a scam. In exchange for a fee it will promise to pester the credit reporting companies until they wipe out your debts and bankruptcy records. It will string you along saying the process will take several months. By then you may be out hundreds or even thousands of dollars. In the meantime, debts can stay on your credit record for up to seven years, and a Chapter 7 bankruptcy can remain for up to 10 years. If you think you were duped by a CRO you should call the FTC Consumer Response Center at **(877) 382-4357**. To keep from being scammed you should avoid any company that does any of the following:

- Wants you to pay for credit repair before they provide any services,
- Will not tell you your legal rights,
- Will not tell you what you can do on your own at no cost,
- Tells you not to contact a credit reporting company directly,
- Advises you to dispute all negative items in your credit report, or
- Suggests you create a new credit identity, e.g., by applying for an Employer Identification Number to use instead of your SSN.

Here are some things you can do to improve your credit.

- Check your credit reports regularly for mistakes or collections you didn't know about. Free copies are available annually from Equifax, Experian, and TransUnion, the three nationwide consumer credit reporting bureaus, by visiting **www.AnnualCreditReport.com** or calling **(877) 322-8228**, a service created by these bureaus. Contact the reporting bureaus in writing about any mistakes or disputed collections. If a mistake is confirmed you can ask the reporting bureau to send a corrected report to prospective lenders.
- Check that past-due accounts older than seven years from the first date of delinquency have been removed. Challenge any that are still on the report. Include copies of documents that support your position and a copy of the credit report. Send them to the reporting company by certified mail.
- Pay down or pay off outstanding debt. Deal with those with the highest interest rates first.
- Develop a plan to pay off high-interest credit card debts. Advice on planning is available from the National Endowment for Financial Education's website at **www.smartaboutmoney.org**. Paying the monthly minimum due is very expensive. It will also take a very long time to pay off the balance. Consider the following alternatives: (1) use savings or investments, especially those that are earning less than the debt interest rate, to pay down the balance, (2) reduce expenses in order to make greater payments, (3) take out a loan at a lower-interest rate to pay off the balance, and (4) stop charging things on the card.
- Try to negotiate a lower interest rate or late fees if you are having trouble paying a debt. Speak to a supervisor who has authority to change the terms of your loan.
- Consider seeing a credit counselor if you can't handle your debts on your own. Consultations are usually free. Two organizations that can refer you to a counselor are the National Foundation for Credit Counseling and the Association of Independent Consumer Credit Counseling Agencies. You can call the former at **(800) 388-2227** or visit its website at **www.nfcc.org**. You can call the latter at **(866) 703-8787** or visit its website at **www.aiccca.org**.
- Get a secured credit card if you need to re-establish your credit. Such a card requires a security deposit to secure your charges to it. And they usually have fees that regular cards do not have. Look for cards with reasonable fees.
- Prepaid debit cards will not help you establish a good credit history because their use is not reported to the three major credit reporting bureaus. Also, be aware that such cards come at a steep price, and while their funds are FDIC insured, the cards aren't protected by federal laws that limit credit card losses to $50 for fraudulent charges. Before buying a prepaid card make sure you know about all the fees and understand the small print in

the cardholder agreement. There can be fees for first-time issuance, reloading, ATM usage,balance inquiries, maintenance, and replacement. This information is usually only available on the company's website. For more information on prepaid cards, see the Consumers Union paper entitled *Prepaid Cards: Second Tier Bank Account Substitutes* dated September 2010 at **www.sdut.us/prepaidplastic**.

These and other things you can do to repair your credit are explained on a page entitled *Building a Better Credit Report* on the FTC's website at **http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre03.shtm#scams**.

Debt Settlement

Debt settlement, a process in which a consumer who is behind in debt payments negotiates with the creditor to pay off the debt in full for less than the amount owed, has become a big business as American consumers struggle with historic levels of unsecured debt. Problems arise when a consumer pays a debt-settlement company to do the negotiations and make the payments. A recent investigation by U.S. Government Accountability Office (GAO) found that some debt-settlement companies engage in unscrupulous activities. (Its report, GAO-10-593T entitled *Debt Settlement: Fraudulent, Abusive, and Deceptive Practices Pose Risk to Consumers* and dated April 22, 2010, can be found online at **www.gao.gov** by searching for its number.) These include:

- Charging fees before settling any debts
- Applying monthly payments to fees before reserving them for debt settlement
- Advertising that their services were linked to government programs
- Offering $100 if they could not get a consumer out of debt in 24 hours
- Claiming high success rates, up to 100 percent
- Suggesting that consumers stop paying on their debts

You can avoid being scammed when seeking help with debt settlement by doing your homework and shopping around. Consider several companies. Check them out with the BBB. Go on the Internet and see what people are saying about them. Find out how long they have been in business and whether any legal actions are pending against them. Ask about their services and fees.
You should also consider debt consolidation, credit counseling, and doing it yourself. The first is a process in which a consumer takes out a load to combine debts into one payment, typically smaller and at a lower interest rate than the individual debts. In the second a consumer receives credit counseling and assistance in managing finances, budgeting, and debt consolidation without a loan. The third involves the following:

- List your goals.
- List your expenses and see which ones you can reduce or eliminate.
- Call your creditors to request a lower interest rate. Do this before your debts are assigned to a collection agency.
- Put as much money as possible to reducing your debt, and keep doing it until all your debts are paid off.
- Sell any stuff you don't use to make extra money.

Dishonest Tax Return Preparers

In this scam dishonest tax return preparers tempt seniors, people with little or no income who normally don't have a tax filing requirement, and members of church congregations to file tax returns claiming fraudulent refunds. The preparers claim they can obtain a tax refund or a stimulus payment for their victims based on the American Opportunity Tax Credit even if the victim was not enrolled in or paying for college. They may charge exorbitant upfront fees and are long gone when their victims discover they've been scammed. Also, the victims will have to repay any refunds the IRS paid before it determined the claims were false. Taxpayers should beware of any of the following to avoid being involved in this scam.

- Unfamiliar for-profit tax services selling tax refund and credit schemes
- Internet solicitations that direct individuals to toll-free numbers and then ask for SSNs
- Flyers and brochures implying tax credits or refunds without proof of eligibility or documentation
- Promises of refunds for persons who don't have to file a tax return

- Claims for Economic Recovery Credit Program or stimulus payments
- Unsolicited offers to prepare a return and split the refund
- Promises of refunds if asked to make false statements of entitlements to tax credits

You can also avoid this scam by wisely choosing a tax preparer. Here is how to do this.

- Check the person's qualifications. All paid tax return preparers must have a Preparer Tax Identification Number (PTIN). Also ask if the person is affiliated with a professional organization and attends continuing education classes. In the future the IRS will require all those not enrolled as an agent, CPA, or attorney to pass a test to become a Registered Tax Return Preparer.
- Check the preparer's history. See if he or she has a questionable history with the BBB, been subject to disciplinary actions by state agencies or professional organizations, and has a current license.
- Avoid preparers who base their fee on a percentage of your refund or claim they can obtain larger refunds than other preparers.
- Have any refund sent directly to you or deposited in your bank account. Never allow it to go to the preparer.
- Make sure the preparer is accessible after your return has been filed in case the IRS questions anything on it.
- Do not use a preparer who does not ask to see all the records and receipts needed to prepare your return.
- Never sign a blank return.
- Review the entire return before signing it. Ask questions and make sure you understand it. And make sure the preparer signs it with his or her PTIN. Although the preparer signs it, you are responsible for the accuracy of every item on your return.
- Get a copy of your return.

Earned Income Tax Credit

This scam targets low-income working families and individuals who: (1) don't have to file federal income tax returns because their gross income is below the filing requirement in Table 1 of Publication 501, (2) qualify for the Earned Income Tax Credit but don't know about it, and (3) haven't filed for the credit. The scammers say they will file for them give them a check for a small amount, say $400. The victims don't realize that if they had filed for credit themselves they would receive more than $400. The scammers make the difference; they also file for credits in prior years. All the victims are asked to do is provide their SSNs and sign the bottom of the form. The scammer then puts his or her address on the form and receives the full credit due. By signing a false form the victims not only lose some credits but may be liable to pay the money back with penalties. Any offer to file for this credit is a scam and be refused. People who qualify for this credit can get free assistance from the IRS at its San Diego Office at 880 Front St. It's open Monday through Friday from 8:30 a.m. to 4:30 p.m. You can call **(619) 615-9555** for an appointment.

Empty Box Bargains

In this scam parking lot or street hawkers offer the hottest electronic gadgets for rock-bottom prices from the back of a truck or van. They'll show you samples of their wares but your purchase will be in a sealed box. When you get home and open it you'll find it empty except for some weights. You can protect yourself from this scam by not buying anything from someone in a parking lot or on the street, no matter how good the price sounds. If the deal sounds too good to be true, it usually is.

Fraudulent Checks

Someone sends or gives you a check and asks you to deposit it in your bank and then wire back a portion of the amount, leaving you with a net profit. This can happen in many ways and will sound like a good deal. But the check will be counterfeit. It will be returned to your bank and the full amount deducted from your account. You can avoid this problem by not cashing the check in the first place, but if you do you should wait until it clears before withdrawing any of it.

In one example of this scam letters are sent to people asking them to participate in a mystery shopping program to help evaluate a certain business in their area. A counterfeit check that appears to come from a government agency is enclosed along with instructions to deposit it in your bank, spend some at the business and provide a written

appraisal of your shopping experience, keep a portion for your work, and wire the balance elsewhere, typically overseas. There are legitimate companies that hire mystery shopping but they usually pay $8 to $20 per shop after the assignment is completed, and don't require any wire transfers.

In another example a collection lawyer receives what appears to be a legitimate solicitation e-mail from a prospective client seeking representation in a debt collection matter. The lawyer then receives what appears to be a valid cashier's check, supposedly a settlement check from a debtor, from a reputable bank. After the check is cashed and the money deposited in the lawyer's client trust account, the "client" asks that the funds, less the fees, be wired to a foreign bank. The cashier's check was fraudulent and the lawyer was left holding the bag.

In January 2007 The Office of the Comptroller of the Currency (OCC) sent out bulletin OCC 2007-2 to all national banks warning them of an increasing number of complaints relating to fraudulent cashier's checks and advising both depositary and paying banks of actions to take to address risks to them. These fraudulent checks have often been received by bank customers who sell goods or services over the Internet. And in some cases they are asked to wire other funds to third parties. In all these case the customer believes the cashier's check to be valid and deposits it in his or her account. When the bank makes the funds "available" the customer sends the goods or funds. Later the check is returned unpaid because it is discovered to be fraudulent. To avoid losses from this check scam bank customers should wait until the check clears before sending goods or funds. The IC3 recommends taking the following steps to determine whether a check is counterfeit:

- Ensure that the amount of the check matches in figures and words.
- Inspect the check to see that the account number is not shiny in appearance, the drawer's signature looks natural, i.e., not traced, and the check is perforated on at least one side.
- Inspect the check for additions, deletions, or other alterations.
- Contact the financial institution on which the check is drawn to ensure its legitimacy. Obtain the phone number from an independent, reliable source, not from the check itself.
- Be cautious in dealing with foreigners.

Free Samples

After using your credit card to pay $5 to cover handling and shipping costs, you receive the "free" sample product you ordered. A few weeks later you receive a larger bottle of the product along with an invoice stating that $75 has been charged to your credit card. By failing to read the cancellation policy in the terms and conditions for ordering the "free" sample, you were enrolled in the company's monthly automatic shipping program.

To avoid "free sample" or "free trial offer" scams be sure to read the terms and conditions carefully. Don't accept an offer if you can't or don't understand them. Also look for pre-checked boxes. They can bind you to terms and conditions you don't want to accept. And look for information about how to cancel future product shipments or services if you don't want them. Do you have to pay? Do you have a limited time to respond? Remember, free rarely means free in Internet commerce. And finally, check your credit and debit card statements after you've responded to a free trial or sample offer. Look for any charges you don't recognize or didn't authorize. If you seen any notify the card issuer promptly and contact the merchant to try to resolve the changes.

Gift Card Stripping

In this scam thieves use an inexpensive scanner to read the code behind the magnetic or scratch-off strip on the back of a preloaded gift card, which along with the number on the front of the card, enables them to steal the value of the card. They return the worthless card to the rack where an unsuspecting customer buys it. Or if the card is not preloaded, the thief can call the 800 number on the card every few days to check the balance and spend it before the customer does. You can protect yourself from this scam by doing the following:

- Don't buy a card that looks like it's been handled or tampered with. If the card comes in a sleeve, make sure it's not crinkled or torn.
- Only buy cards that are behind a customer-service desk.
- Ask the cashier to scan a preloaded card to make sure the full value is on it.

Green Dot MoneyPaks

MoneyPaks are reloadable debit cards that can be used to pay for goods or services. They work just like cash and transactions with them cannot be traced or reversed. If a business only accepts payment this way, it's probably a scam. So use MoneyPak only to reload prepaid credit cards or accounts you control. And never give your MoneyPak number to someone you don't know.

Green Energy Conservation

With billions in stimulus money being released by the Federal Government for green energy programs, millions of Americans are considering home improvements that will save energy and give them tax credits of up to $1,500. To avoid being victimized by scammers who are trying to cash in on this, homeowners should keep the following in mind.

- Not all improvements qualify for tax credits. Those that do qualify are listed on **www.energystar.gov/taxcredits**.
- Do not accept any offer to file the "necessary paperwork" for a fee. You can easily do it yourself.
- Ignore any e-mail from the U.S. Department of Energy promising a refund. And don't open its attachment, which could unleash malware in your computer.
- Don't let any people into your home to do energy audits or make energy-saving repairs. Scammers often pose as local utility company employees to do this. In taking advantage of legitimate rebate programs, call the company first to set a time for an employee come to your home.
- Don't fall for high-pressure sales pitches for energy-saving devices. They don't work.
- Beware of unscrupulous contractors. See the separate section above on ways to avoid their scams.

Healthcare Fraud

The passage of the 2010 health insurance reform bill has provided scam artists and criminals with an opportunity to confuse and defraud the public by selling phony insurance policies. Scammers are now going door to door in some areas urging consumers to obtain coverage in a non-existent "limited-enrollment" period that they falsely state was made possible by the new legislation. They are also setting up toll-free phone numbers and using the Internet to sell phony policies and threaten people that they will go to jail unless they have health insurance. Consumers need to inform themselves about the new legislation and the availability of new options. They should also check whether the insurance company and the person selling the insurance are licenses, as suggested above in preventing predatory insurance sales practices. Also, any person selling door to door should be wearing a SDPD-issued photo-ID registration card. Solicitors without this card should be reported to the SDPD on its non-emergency number, **(619) 531-2000** or **(858) 484-3154**.

There is a wide variety of other healthcare scams. Without going into detail about each one, here are some ways to protect your healthcare benefits.

- Treat your Medicare, Medi-Cal, and SSNs like credit card numbers. Never give them to a stranger. And don't carry cards unless you will need them that day.
- Medicare doesn't call or visit to sell you anything.
- Don't accept offers of money or free food or gifts for medical care. Watch out for incentives like "it's free" or "we know how to bill Medicare."
- Keep a record of your doctor visits, tests, and procedures so you can check to see if Medicare or Medi-Cal is being charged for something that didn't occur.
- Check your medical bills and explanations of Medicare benefits for mistakes. Look for charges for services or products you didn't receive, billing twice for the same thing, or bills for services not ordered by your doctors. Your Medicare account records are available on line at **www.MyMedicare,gov**.
- Contact your provider or plan first if you see any errors. There may have been a simple mistake.
- If you suspect Medicare fraud, call the Office of the Inspector General of the U. S. Department of Health & Human Services at **(800) 447-8477** or send an e-mail to **hhstips@oig.hhs.gov**.
- If you suspect Medi-Cal fraud, call the California Department of Health Care Services Medi-Cal Fraud Hotline at **(800) 822-6222**.

High-Pressure Sales of Financial Products at Free-Meal Seminars

Many financial services firms sponsor sales seminars and offer a free meal to entice attendees. While these seminars are advertised as educational workshops at which "nothing will be sold," they are actually held to get attendees to open accounts and buy investment products, if not at the seminar itself, then in follow-up contacts. In a 2007 study of these seminars by the U.S. Security and Exchange Commission, the Financial Industry Regulatory Authority, and state securities regulators, it was found that about half featured exaggerated or misleading advertising claims and about one-quarter involved unsuitable investment recommendations. Attendees need to understand that these seminars are primarily sales events and that all claims and recommendations should be evaluated with great care before taking any actions.

Immigration Scams

Navigating U.S. immigration laws can be complex. Missing a deadline or choosing the wrong form can jeopardize a person's immigration status, or make it harder to legally remain in the United States. Unauthorized immigration services providers and scam artists look for ways to exploit immigrants, and often take their money while doing nothing for them. Unauthorized providers may also lose important documents, provide substandard service, or encourage immigrants to make false statements to the government. The result can be rejection or denial of benefits and, in some cases, criminal prosecution. They might also use the personal information you provide to steal your identity.

Choosing the right person to help you is almost as important as filling out the right form, or filling it out the right way. The help that you see advertised in store windows, on websites, in the newspaper, on the radio can hurt you. People who call themselves immigration consultants or experts, or *notarios* cannot help you. Even people who mean well – a friend, your pastor, a teacher, or a relative – can cause problems for you later. Helpers like these should only write or translate what you tell them to, not give you advice on what to say or which forms to use. To get real help you should work with people who are authorized by the U.S. government to help you. They will help protect you from people who will cheat you.

Dishonest people sometimes charge for blank government forms, say they have a special relationship with the government, or guarantee to get you results. They may promise to get you a winning slot in the Diversity Visa lottery if you pay a fee. They might charge a lot of money, supposedly to guarantee temporary protected status or get you benefits you don't qualify for. They are very clever about finding ways to cheat people.

Because immigrants with limited English language proficiency often are targeted by scammers the FTC has developed education materials in English, Spanish, Chinese, and Korean. These materials explain how to avoid and report immigration scams and how to find legitimate no-cost or low-cost immigration advice from authorized providers. They can be downloaded from the FTC's website at **www.ftc.gov/bcp/edu/microsites/immigration/index.shtm**.

Here are some ways to avoid these scams.

- Don't go to a *notario, notario público*, or a notary public for legal advice. Although some notaries might also be attorneys, i.e., lawyers that are members of The State Bar of California, they are not allowed to give you legal advice when acting as a notary. And as such they cannot talk the U.S. Citizenship and Immigration Service (USCIS) or the Board of Immigration Appeals (BIA) on your behalf. Ways to get the right help are listed below.
- If you use the Internet you can get immigration information and forms from the U.S. Citizenship and Immigration Service (USCIS) website at **www.uscis.gov/portal/site/uscis**. You can download forms there for free, though you'll probably have to pay when you submit them to USCIS. Unauthorized service providers and scammers usually design their websites to look official. Their URLs end in "**.com**." They will charge you for forms and other services.
- If you don't use the Internet you can get free immigration forms by calling USCIS at **(800) 870-3676**, or by visiting the USCIS field office in San Diego at 880 Front Street.
- Don't let anyone keep your original documents, like your birth certificate or passport. Scammers may keep them and charge you to get them back.

- Never sign a form before it has been filled out, or a form that has false information in it.
- Never sign a document that you don't understand.
- Keep a copy of every form that you submit, as well as every letter from the government about your application or petition.
- Keep the receipt you'll get from USCIS when you turn in your paperwork. It proves that USCIS received your application or petition. You will need the receipt to check on the status of your application.

To find an immigration lawyer who provides free or low-cost legal services for immigrants and refugees:

- See the list of free legal service providers in California on the U.S. Department of Justice website at **www.justice.gov/eoir/probono/states.htm**.
- Call USCIS at (800) 375-5283 to ask about lawyers in your area.
- See the Immigration Legal Service Providers Directory by state on the American Bar Association's website at **www.americanbar.org/groups/public_services/immigration/resources/immigration_legal_service_providers_directory.html**

To obtain free legal advice or representation:

- Contact a local law school. Law students can give you legal advice if they are supervised by a lawyer or accredited representative.
- Find someone in your community known to USCIS as a "reputable individual" to represent you. They have to sign a legal document saying they won't take money from you.

To find a lawyer in your area who works in immigration but will charge a fee to help you:

- Visit the website of the American Immigration Lawyers Association at **www.ailalawyer.com**. There you can also get answers to many frequently asked questions, including ones about the costs and qualifications of an immigration lawyer.
- Visit the website of the State Bar of California at **members.calbar.ca.gov/search/ls_search.aspx** to conduct a legal specialist search. Select Immigration & Nationality Law and San Diego County from the drop-down menus to get a list of certified specialists.

To check to see if someone is actually a lawyer, and to find out if a lawyer has been disciplined, suspended, or expelled by the State Bar:

- Visit the website of the State Bar of California at **www.calbar.ca.gov** and enter the person's name in the Attorney Search box to see the person's bar membership record.
- Visit the U.S. Department of Justice's website at **www.justice.gov/eoir/discipline.htm** to see a list of currently disciplined practitioners.

Another group of people who are authorized by the U.S. government to give legal immigration advice and represent you are called accredited representatives. They are not lawyers work for an organization that's officially recognized by the U.S. government. They may charge a fee to help you. Both the accredited representatives and these recognized organizations are on a list kept by the Board of Immigration Appeals (BIA) at the U.S. Department of Justice. You can see this list by state on the U.S. Department of Justice's website at **www.justice.gov/eoir/statspub/raroster_files/raroster_orgs_reps_state_city.htm**.

Investment Opportunities

Investment pitches come by phone, postal mail, e-mail, newspaper and magazine advertisements, TV "infomercials," etc. They can also come from friends, relatives, co-workers, neighbors, and members of groups or organizations you belong to. Some may be legitimate, but many are scams designed to separate you from your money. Remember, scam artists are skilled liars. They are usually very friendly, very good at sounding like they represent legitimate businesses, and have believable answers to any questions you may ask. And they often prey on seniors, widows, fellow members of ethnic or religious groups, or cultural or community organizations whose trust they betray. The following tips will help you spot and avoid most types of investment scams:

- Don't believe claims that there is no risk. All investments, even legitimate ones, involve some risk. Never invest more than you can afford to lose.
- Be wary of promises that you will make a good return fast. Legitimate investments require time to pay off. If the offer sounds too good to be true, it probably is. Be highly suspicious of any "guaranteed' investment opportunity.
- Be suspicious of an investment in which regular, positive returns are promised regardless of the overall market conditions. Investment values tend to go up and down over time, especially those with high returns.
- Never rely solely on unsolicited investment information from an e-mail or fax, especially when the sender makes extravagant claims about its future value. Be skeptical whenever you receive a stock tip. Tipsters try to get you and others to buy the stock so the price will go up and they can sell off their shares at the inflated price.
- Check the source of any message you receive because it may come from a company insider who is paid to advertise the stock.
- Don't be fooled by testimonials offered by strangers. Often these are fictitious or made by the scammers to encourage you to invest.
- Avoid investments you don't understand or for which you can't get complete information. Understand what you are investing in and how your investment will be held or managed. If you are unsure about anything, discuss the investment with your attorney, accountant, or any other licensed professional before you invest. You should also discuss it with your family and trusted friends.
- Don't be afraid to ask questions. Any legitimate business will be glad to answer them.
- Be wary of any business that does not have a street mailing address and phone number.
- Be sure to get everything in writing. Chances are you won't get what was promised otherwise.
- Read the investment's prospectus and disclosure statement carefully before you invest.
- Ask what recourse you would have if you are not satisfied with your investment or if you need to get your money out quickly. It is essential to get any warranty or refund provision in writing, and be confident that the business will honor its guarantees should that become necessary.
- Be suspicious if you don't receive a payment or have difficulty cashing out your investment.
- Be wary of salespeople who promise to "take care of everything" for you. Honest salespeople will make sure you understand the investment. They will also keep you informed about it so you can make appropriate decisions in the future.
- Don't get taken in by offers that are available right now. Don't get pushed into making a quick decision. Take time to think about it, do some research, and discuss it with others. If you are not interested, just say so; it is not impolite to simply say "no" or hang up the phone.
- Be wary of salespeople who ask you to send cash or transfer money immediately, or offer to send someone to pick it up.
- Never pay for something that is "free." Whatever you receive will probably be worth less than what you've paid for it.
- Never meet with a salesperson alone in your home.
- Don't disclose your financial situation of provide any personal information such as your SSN or credit card number until you are confident that you are dealing with a legitimate salesperson and company. Never give out personal information for "identification" purposes.
- Check the credentials and licensing of any salesperson, broker, or other person before investing. Don't deal anyone who isn't licensed.
- Ask what state or federal agencies the salesperson's firm is regulated by and with whom is it registered. Get the phone number and URL so you can contact the agencies to verify the facts. Don't deal with salespeople who say their firm is not subject to registration or regulation.
- Don't consider investments that are not registered with the U.S. Securities and Exchange Commission (SEC) or a state regulator.
- If the investment involves securities, you can go to the Financial Industry Regulatory Authority's website at **www.finra.org** and look up the status of brokers or brokerage firms on its BrokerCheck on its Investors page. You can also get a detailed report that includes the firm's profile, history, operations, and disclosure events. The latter include arbitration awards, disciplinary actions, bankruptcies, etc. Also check with the California Department of Corporations at **www.corp.ca.gov** or **(866) 275-2677** to verify that the company offering stock or other securities is registered, and that the investment opportunity is legitimate and legal. And you can see company's quarterly and annual reports on the SEC's website at **www.sec.gov** under Filings & Forms.
- Ask for the name of the firm your investments clear with.

- If the investment involves commodity futures, you can go to the National Futures Association's website at **www.nfa.futures.org** and look up the status of individuals or firms on its Broker/Firm Information (BASIC) page. You can also go to the Commodity Futures Trading Commission's website at **www.cftc.gov** and look up the disciplinary history of individuals or firms under Consumer Protection.
- Be wary of any individual or firm who offers to sell you commodity futures or options on commodities, particularly precious metals, foreign currency, and those with seasonal demands. These investments are very risky and anyone who claims otherwise may be breaking the law.
- If you have a self-directed IRA, i.e., one in which you can hold alternative investments such as real estate, mortgages, tax liens, precious metals, and unregistered securities, you cannot depend on the custodian to investigate and validate your investments or any financial information provided about them. Custodians are only responsible for holding and administering the assets in the IRA. And they have no responsibility for investment performance. This puts the burden on you to avoid Ponzi schemes and other frauds. For ways to avoid these dangers see the investor alert published by the SEC Office of Investor Education and Advocacy at **www.sec.gov/investor/alerts/sdira.pdf**.
- Be wary of investment offerings involving distressed real estate. Investments in properties that are bank-owned, in foreclosure, or pending short sales carry substantial risks and should be evaluated carefully. And as with other securities, interests in real estate ventures must be registered with state security regulators. For ventures in California you can check licenses on the California Department of Real Estate's website at **www.dre.ca.gov/gen_lic_info.html**. Click on button entitled California Real Estate & Financial Services License Information to get a page entitled Multiple Department License Lookup. You will then be able to search for licenses issued to persons and companies by the Department of Real Estate, the Office of Real Estate Appraisers, the Department of Corporations, and the Department of Financial Institutions, which regulate most of the real estate and financial services in California.

Job Offers

Persons looking for jobs need to be aware of scammers who are asking for personal information and upfront money for help in finding a job. They keep the money and use the personal information for identity theft. The following red flags warn you of a likely job scam:

- The employer offers the opportunity to become rich without leaving home. While many legitimate businesses allow employees to work from home, many scammers try to take advantage of seniors, stay-at-home moms, students, injured or handicapped people, and those otherwise unemployed. They often require an upfront investment in office supplies and other materials and then fail to deliver the salaries promised. Legitimate businesses that offer work-at-home arrangements typically pay from $8 to$15 an hour. These jobs involve low risks and have low rewards.
- The employer asks you to receive packages at your home or business and mail them to someone else, usually out of the country. These packages contain merchandise bought with stolen credit cards. If you reship them you become part of a smuggling operation and can be arrested and charged with mail fraud, etc.
- The employer or a placement agency asks for upfront money. Scammers will say upfront money is needed for background checks or training for jobs that don't exist.
- The salary and benefits offered seem too good to be true. Phony employers will promise high salaries and good benefits for little work with no experience necessary.
- Employer e-mails are full of grammatical and spelling errors. They usually come from scammers outside the U.S. where their first language isn't English.
- The employer requires you to get a credit report from a recommended website. This is an attempt to get personal financial information or sell you credit monitoring services.
- The employer asks for personal information before you get the job. This is an attempt to get your Social Security and bank account numbers.
- The employer sends you a check and asks you to wire a portion back. These checks are not good. If you cash them your bank will ask you to pay them back when the check does not clear the bank is written on.

Before dealing with any company that offers you a job, especially by e-mail, do some research on the company. First find out where it is based. Don't have anything to do with a company that has a Post Office box for an address. Then do a search of the records in the state in which it is incorporated or registered to verify any information provided. And check it out with the BBB at **www.bbb.org**.

Landlord Impersonation

In this scam, which has become more frequent as the number of vacant and foreclosed homes increases, a person pretending to be the property owner rents a home to a prospective tenant and asks for first- and last-month's rent and a security deposit in cash. All this money will be lost and the "tenants" can be evicted when the real property owner shows up. Before renting, prospective tenants should call the San Diego County Assessor's Office to make sure the person renting the property is the real owner. You can call its public information number, **(619) 236-3771**, on weekdays from 8 a.m. to 4 p.m. to get the property owner's name.

Medicare Enrollment

Seniors should be on the lookout for Medicare scams especially during the open enrollment period that runs from November 15 to December 31 each year. The scammers will try to obtain your personal information or sell you a plan that's not the best fit your needs.

You can protect yourself by doing the following:

- Don't give out personal information to anyone claiming to be from Medicare. It already has that information. However, it is all right to provide Medicare information if you have initiated a call to Medicare for assistance, or to Medicare-plan provider when you choose to enroll in a plan.
- Be wary of brokers who try to pressure you into enrolling in a specific plan. Medicare-plan providers aren't allowed to make cold calls or come to your door unless they are invited. And don't believe claims that a plan is "Medicare Endorsed" or that you will lose benefits unless you enroll in a specific plan.
- Research and verify plans with Medicare by calling **(800) 633-4223** or going to **www.medicare.gov**.

Post-Foreclosure Solicitations

Tenants in foreclosed homes and former homeowners who remain in them may be solicited by persons or companies promising to help them stay in the home and avoid eviction. The dangers are that the solicitor is not licensed, doesn't know the law, is behaving unethically, or takes an advance fee and fails to provide any services. Solicitations by attorneys cannot be threatening, e.g., saying "if you do nothing you risk eviction in 15 to 30 days," raise false hopes or guarantee the result of the representation, or be made in person or by phone. And if by mail, they must bear the word "Advertisement." Real estate agents must act fairly and honestly with respect to the transaction. Misrepresentations, harassment, failure to disclose material information or advise the person in the home of his or her rights with respect to eviction as a result of foreclosure, or negligence could possibly lead to disciplinary action.

Solicitations are legal as long as the solicitor is licensed. You can check real estate licenses on the California Department of Real Estate's website at **www.dre.ca.gov/gen_lic_info.html**. Click on button entitled California Real Estate & Financial Services License Information to get a page entitled Multiple Department License Lookup. You will then be able to search for licenses issued to persons and companies by the Department of Real Estate, the Office of Real Estate Appraisers, the Department of Corporations, and the Department of Financial Institutions, which regulate most of the real estate and financial services in California. You should also check that a company is licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. You can check this in the business listings on the City's website at **http://www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml**. For legal services you need a licensed attorney. Real estate agents or companies cannot offer legal advice. You can check whether a person is a licensed attorney and see his or her membership record on the California Bar's website at **www.calbar.gov**. After checking licenses you should go to the BBB website at **www.sandiego.bbb.org** to see the company's record with it.

After all this checking you should ask whether the advance fee covers just advice, i.e., a consultation, or advice and services. And if the latter, ask whether the solicitor is licensed to provide them and what services will be provided. Also ask what additional services might be involved and what they would cost.

Predatory Insurance Sales Practices

These practices involve insurance agents holding informational meetings or seminars about finances, living trusts as a way to avoid probate, or insurance investments that guarantee you will not outlive your retirement savings. These sessions are often held in senior centers, religious institutions, and restaurants. Attendees are required to sign in and give the agent their names, addresses, and phone numbers. Sometime after the session the agent, who may claim to be a "specialist" or "advisor," will contact the attendees to set up a meeting in their homes. It is in these one-on-one meetings that attendees can get pressured into buying an insurance product that is completely inappropriate for their needs. If you attend one of these information sessions you should not give any personal information to the agent. And you should talk to a trusted advisor before making any changes in your investments and insurance. Beware of limited-time offers and other tactics used to force you into a quick decision.

Although the vast majority of life insurance agents are honest, there are some who take advantage of persons whose trust they have gained, especially seniors, and take money from them to buy unnecessary insurance or annuities with promises of high returns. In some cases these financial predators convert the money to their own use.

To prevent this fraud you should first check the agent's license. It is required to be printed on all business cards, quotes, and advertisements. You can check it on the California Department of Insurance (CDI) website at **www.insurance.ca.gov**. Look under Agents & Brokers for the page entitled Checking License Status. You can check by name or license number. You should also check out the insurance company. In the CDI website look under Seniors on the page entitled Before You Buy Insurance and click on Check out the Insurance Company to verify that it is authorized to conduct business in California. You can also get this information by calling the CDI at **(800) 927-4357** between 8 a.m. and 5 p.m. Monday through Friday.

Then for the sale of a life insurance or annuity policy in your home, you must receive a written notice from the agent at least 24 hours before the meeting. The notice must include the reason for the meeting, and the names, license numbers, and phone numbers of all persons coming to your home. It must also state that: (1) others are invited to attend, e.g., family and friends, (2) you have the right to end the meeting at any time, (3) you have the right to contact the CDI for more information or to lodge a complaint, and (4) prior to purchase of a life or annuity policy you are entitled to a full disclosure of all surrender charges and related time frames in connection with the purchase. You must also be provided with all information relating to benefits and negative consequences regarding the replacement of an existing policy or annuity.

If you purchase a policy or annuity, you then have 30 days to review it, and it you return it by the 30th day after you receive it, you are entitled to a full refund of your premium in a timely manner. If you believe you've been the target of insurance fraud, call the CDI consumer hotline at **(800) 927-4357** between 8 a.m. and 5 p.m. Monday through Friday.

Insurance agents also prey on military personnel before they deploy overseas. They take advantage of the emotional situation of leaving families at home and try to sell extremely overpriced or misrepresented life insurance policies. Military personnel desiring additional coverage should buy Service members Group Life Insurance (SGLI), which is a legitimate source for low premium policies. Service members have no need to by private insurance.

Prize Notification and Lotteries

In this scam a person is notified by e-mail, letter, or fax that he or she has won a prize and told to send the contest or lottery sponsor a signed release form and money to cover various expenses before the prize can be awarded. You lose not only the money but may provide the scammer with information for use in stealing your identity and committing various other financial crimes. Never respond to such a notice. Real prize winners don't have to pay a fee or taxes up front. If the notice came by mail, report the scam to U.S. Postal Inspector at **(877) 876-2455**.

In the case of lotteries, it is a federal crime to participate in a foreign lottery by mail, i.e., to send solicitations or payments for tickets. Most all foreign lottery solicitations sent by mail to U.S. addresses come from scam artists. Discard any you might receive. And don't provide any personal information. You can't win no matter what they say.

Property Tax Relief

Some companies have been offering to help homeowners reduce their property taxes for an up-front fee and not performing any reassessment or reassessment-appeal services. Their mailers featured official-looking logos and warned homeowners that their files would by ineligible for tax reassessments if they did not respond by a certain date. Homeowners should be wary of such solicitations and consider filing for property tax relief themselves. There is no cost for this. The procedure is explained on the website of the County Assessor/Recorder/County Clerk at **http://arcc.co.san-diego.ca.us**. Click on Reassessment/Ownership under Assessor Services, then on Proposition 13, and then on Application for Review of Assessment in the answer to the question: Can the assessed value of my property be decreased? You will get a page entitled "Property Tax Relief" and an Application for Review of Assessment. For additional information you can call the County Tax Assessor at **(858) 505-6262**.

Reverse Mortgages

Abuses and abusers from the subprime mortgage market are now appearing in the home equity conversion (reverse) mortgage market, putting the equity and savings of millions of seniors at risk That's the main finding of a report issued by the National Consumer Law Center (NCLC) in October 2009. This report can be read on the NCLC website at **www.nclc.org** by looking under Issues, then Foreclosures and Mortgage Issues, and then Predatory Mortgage Lending. Click on the report entitled *Subprime Revisited: How the Rise of the Reverse Mortgage Lending Industry Puts Older Homeowners at Risk*. In many of these reported scams seniors are offered investment opportunities, foreclosure rescue, refinancing assistance, or free homes. They are recruited through local churches, investment seminars, direct mailings, and radio, TV, and other advertising. Seniors should do the following to avoid becoming a victim of these scams:

- Do not respond to unsolicited ads for reverse mortgages or proposals for investing the proceeds from these mortgages.
- Make sure that any private professional fiduciary who handles your assets has a valid license from the California Department of Consumer Affairs Professional Fiduciaries Bureau.
- Make sure your lender follows all the requirements of California Assembly Bill 329, the Reverse Mortgage Elder Protection Act of 2009. Except as specified, this Bill prohibits lenders from associating with any party that is associated with any other financial or insurance activity, and from referring the borrower to anyone for the purchase of an annuity or other financial or insurance product prior to the closing of the mortgage or the expiration of the right of the borrower to rescind the mortgage agreement. It also requires the lender to provide the borrower with a list of at least 10 counseling agencies in California approved by the U. S. Housing and Urban Development (HUD), and a checklist of issues the borrower should discuss with a counselor. One issue is whether the prospective borrower's financial needs would be better met by other options like a less costly home equity line of credit. The checklist must be signed by the counselor and provided to the lender before the loan is approved. The lender is also required to inform the borrower that senior advocacy groups advise against using the proceeds of the mortgage to purchase an annuity or related financial products without discussing the financial implications with your counselor and family. These advocates have long cautioned that reverse mortgages should be a last resort because of their higher fees.
- Do not sign anything that you do not fully understand.

Short Sales of Homes

A short sale is an alternative to a foreclosure, which is a more time-consuming and costly process for the lender and the homeowner. In it the lender allows the homeowner to sell the property for less than what is owed on the existing mortgage and agrees to forgive some or all of the debt. The scam occurs when the agent or short-sale negotiator, who was hired by the homeowner, receives several bids but submits only the lowest. Unaware of higher bids, the homeowner and the lender accept that bid. This has the following effects. The lender loses the difference between the lowest and highest bid. The homeowner has a greater tax liability because he or she will be taxed on the difference between the debt and the sales price. And the crooked agent or short-sale negotiator, who is also working with the lowest bidder, sells the property to the highest bidder and makes a sale profit in additional to his commission.

Because of the possibilities of fraud, tax liabilities, and suits by the lenders to recover the forgiven debt, before you decide to sell through a short sale you should get: (1) a licensed and qualified real estate agent to represent you, (2) the advice of an accountant, and (3) the advice of an attorney. And then you need to look out for the following:

- Any short-sale negotiator must be a licensed real estate broker or a licensed real estate salesperson working under the supervision of a broker.
- Real estate licensees wishing to collect an advance fee must first submit an advance fee contract to the California Department of Real Estate and receive a no-objection letter for that contract. Then any advance fees paid must be placed in a trust account and handled as client trust funds.
- All payments must be fully disclosed and made a part of the escrow documents. Any fees paid outside of escrow are illegal.
- The buyer is a fictitious person or entity, or the buyer is purchasing the property under a power-of-attorney or limited liability company. This may indicate fraud.
- An unlicensed negotiator is handling the sale. This is illegal.

Tax Debt Relief

Beware of attorneys, accountants, and others who offer to make your IRS tax debt vanish for an upfront fee. Most of the time it's your money that vanishes, leaving you with a larger debt as IRS interest and penalties continue to grow. If you owe back taxes or have a tax debt you cannot pay, contact the IRS as soon as possible. There are several programs for taxpayers who cannot afford to pay their debts. These include the following:

- Offer in Compromise, wherein taxpayers make an offer to pay less than the amount owed.
- Installment Agreement, wherein taxpayers pay in monthly installments.
- Currently Not Collectible, wherein the tax debt is postponed until the taxpayer's financial situation improves.

Applying for these programs is free. More information is available online at **www.irs.gov**. You can also get help from the Taxpayer Advocate Service (TAS), an independent office within the IRS. It offers free, independent, and confidential assistance to taxpayers who are unable to resolve their tax problems through normal channels or are experiencing financial hardships. The nearest TAS office is in Laguna Niguel. You can call **(949) 389-4804** for an appointment.

Third-Party Telephone Bill Charges

This telemarketing scam involves the sale of some kind of service. The caller gets you to say "yes" to some question and then mails you information about the service. The mailing looks like junk mail and the caller hopes you will throw it away without reading it because it says that you have some period of time to cancel the service. When you fail to reply, a monthly service fee is added to your phone bill. If you dispute the fee the caller will produce an edited version of the phone conversation in which you agreed to receive information about the service and pay the monthly fees. To avoid the resulting problems you should do the following:

- Hang up immediately on any unsolicited callers. Don't get involved in a conversation. And never say "yes" to any question.
- Open all mail, even if it looks like junk mail. There might be something you need to do to prevent being billed for some service you didn't request or don't need.
- Examine your phone bill for third-party charges. Don't pay any that you did not authorize and report them immediately to the phone company.

Timeshare Transactions

You need to be careful when you buy or sell a TimeShare (T/S). Scams exist in both of these transactions. Beware in buying a T/S if you are told any of the following:

- Your T/S is an investment that will increase in value.
- You can rent your T/S to make money.
- Your maintenance fees will not go up, but if they do, it will only be by a small amount.

- This special sales offer is only good today.
- The sales presentation will only last 90 minutes
- The company will buy your previous T/S for a great profit to you.
- You can go anywhere in the world whenever you want.
- You have a legal right to rescind or cancel the contract whenever you chose.

If you sign a contract to buy a T/S and later have regrets, beware of "attorneys" who offer to get you out of your contract. They will want an upfront fee and will probably do no more than send a letter to the T/S seller demanding that the contract be cancelled.

Most scams occur when you try to sell a T/S. These usually involve some sort of an upfront fee paid to a company who says it will help you sell your T/S. It may say it has a buyer already, it just sold one like yours and knows its market value, or it guarantees to sell yours. Then it asks you will pay an upfront fee for its work. It will also say your fee is refundable if your T/S doesn't sell. Once the fee is paid, the company disappears. You should never pay an upfront fee. And if you want to recover your upfront fee, beware of "attorneys" who offer to help for another upfront fee.

In a variant of this scam the company offers to take your T/S off your hands for an upfront fee so you won't have to continue paying its maintenance fees. All it does is change the address where the maintenance bills are sent so you think there was a transfer of ownership. You are still responsible for those fees.

Another scam involves a company that says your T/S's worthless but offers to buy it for a small amount. The company also says that you will no longer have to make payments on the T/S, and that your loss is tax deductible. Then the company offers to sell you a worthless travel club membership for more than it's paying for your T/S. If you agree to buy it you end up paying the difference, giving up your T/S, which the company can sell for an additional profit, and not getting the promised tax benefit.

Then there's the scam in which a buyer gives you a cashier's check for more than the sales price and asks you to deposit it in your bank and wire back the difference. When the check is found to be counterfeit it will be returned to your bank and the full amount deducted from your account. You can avoid this problem by not cashing the check in the first place, but if you do you should wait until it clears before withdrawing any of it. See the section above on fraudulent check for more about this kind of scam.

If you are considering reselling a T/S, you should:

- Beware of any unsolicited communications.
- Beware of any company that asks for upfront fees.
- Make sure the person offering to list and resell your T/S is a licensed real estate broker or a licensed sales person working for a licensed broker. You can check license numbers and disciplinary actions on the California Department of Real Estate website at **www.dre.ca.gov**.
- Ask for a list of past T/S customers who I can contact as references.
- Ask what the company will do to market your T/S.
- Read the fine print in any sales contract or rental agreement. Get a copy of it.
- Check with the BBB to ensure that the company is reputable.

For more information on T/S resales go to the Timeshare Resales page on the American Resort Development Association – Resort Owners Coalition's website at **www.arda-roc.org/roc/resource-library**.

Unscrupulous Contractor Scams

These are characterized by the following:

- Door-to-door solicitations to do work at a reduced price. Once payment is made little or no work is done and the project is abandoned.
- Pressure for an immediate decision leaving no time to get competitive bids, check licenses, or contact references.

- Offer to perform a free inspection in which non-existent problems are found.
- Demand for immediate payment in cash. Unscrupulous contractors will take the money and run.
- Illegally large down payments. By law a down payment cannot exceed the lesser of 10 percent of the project price or $1,000. See California Business and Professions Code Sec. 7159.5(a)(3).
- Verbal agreements instead of a written contract.

Any suspicious solicitations should be reported to the SDPD at **(619) 531-2000** or **(858) 484-3154** with a description of the person and his or her vehicle license plate number. You can avoid scams in hiring a contractor by doing the following:

- Beware of persons going door-to-door in your neighborhood, having an "office" is his or her vehicle, or driving a vehicle with out-of-state license plates.
- Deal with and hire only licensed contractors. Anyone performing home improvement work valued at $500 or more must be licensed by the Contractors State License Board (CSLB). Get the contractor's license number and verify it online at **www.cslb.ca.gov** or by calling **(800) 321-2752**. The contractor should also be licensed to work in the City of San Diego, i.e., that it has a Business Tax Certificate. You can check this in the business listings on the City's website at **http://www.sandiego.gov/treasurer/taxesfees/btax/nblactive.shtml**.
- Ask to see a photo ID to verify who you are dealing with.
- Get an estimate in writing and make sure you completely understand its terms. It should include a detailed description of the work to be done, materials to be used, total cost and payment schedule, and start and completion dates.
- Get at least three bids and references from each contractor, and check the contractor's references. If possible, go see the contractor's work.
- Confirm that the contractor has a Workers' Compensation policy for its employees.
- Make sure that the contractor is insured. Insurance will protect you from damage caused by the contractor's employees. And consider requiring a surety bond that will guarantee that the work will be performed as stated in the contract.
- Get the contract in writing and don't sign anything until you completely understand its terms. The contract should include a detailed description of the work to be done, materials to be used, total cost and payment schedule, and start and completion dates.
- Check with other lenders before allowing the contractor to arrange the financing for the job.
- Take your time in making a decision.
- Make sure a contract, if signed in your home, contains a three-day right to cancel provision with an attached notice of cancellation form that explains this right. If the contract is for the repair or restoration of residential premises damaged by a disaster, i.e., any sudden or catastrophic event for a state of emergency has been declared by the President of the United States or the Governor, or for which a local emergency has been declared by the executive officer or governing body of any city, county, or city, and county, you have a seven-day right to cancel. These rights are defined in California Civil Code Sec. 1689.7.
- Don't pay cash and not more than the legal limit for a down payment. Beware of contractors who won't accept a check or who wants the check made out to him or her instead of the company.
- Don't let payments get ahead of the work.
- Don't make the final payment until you are satisfied with the work.
- Keep a file of all papers relating to the project, including payments.
- Go to the Guides and Pamphlets page of the CSLB website for more information about safe contracting.

Also, any contractor who is hired to remodel a home built before 1978 must be licensed and certified for lead safety by the U.S. Environmental Protection Agency (EPA). The contractor is also required to provide you with an EPA brochure on the lead safety before starting work. That brochure is available online at **www.epa.gov/lead/pubs/renovaterightbrochure.pdf**. If you remodel your own home you should refer to that brochure for precautions to take to reduce exposure to lead and asbestos during the remodeling.

Another common contractor scam begins with a low-cost air duct inspection or cleaning. A dishonest contractor may then say your ducts are filthy and contaminated with black mold, which costs about $500 to kill with ultraviolet light. Others may also suggest that you need a complete furnace or air duct cleaning which costs about $400, and a replacement air filter that costs over $100. The U.S. Environmental Protection Agency says that most

air duct cleaning is unnecessary. Dust can collect on the air returns but they can be vacuumed easily. And filters can be replaced inexpensively. The whole job should cost less than $75. Any service costing more than a few hundred dollars is probably a scam. Men who do this often arrive in an unmarked vehicle, don't wear a company uniform, use high-pressure sales techniques to scare you, and leave without providing a receipt for work done.

SAFER USE OF THE INTERNET

There are presently two similar efforts by the U.S. Government to promote safer use of the Internet. The one by the FTC's Bureau of Consumer Protection is called *Stop.Think.Click*. The other, developed by a group representing industry, government, academia, and the nonprofit sector in 2009, and promoted by the Obama administration and the Department of Homeland Security is called *Stop.Think.Connect*.

Stop.Think.Click

This effort defines seven practices for safer computing and provides tips on preventing identity theft, safe use of social networking sites, online shopping, Internet auctions, avoiding scams, and wireless security. It also provides a glossary of terms. The seven practices are:

1. Protecting your personal information
2. Knowing who you're dealing with
3. Using anti-virus and anti-spyware software, as well as a firewall
4. Setting up your operating system and web browser software properly, and updating them regularly
5. Protecting your passwords
6. Backing up your important files
7. Learning who to contact if something goes wrong online.

Go to **www.ftc.gov/bcp/edu/pubs/consumer/tech/tec15.pdf** for information about these practices and tips.

Stop.Think.Connect

This effort suggests that users do the following:

- Stop. Before you use the Internet take time to understand the risks and learn how to spot potential problems
- Think. Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact the safety of yourself and your family.
- Connect. Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer.

You can learn how to become a partner in this effort by going to its website at **www.stopthinkconnect.org**. This site also contains the tips and advice for doing the following.

Keeping a clean machine:

- Have the latest security software, web browser, and operating system.
- Use programs that automatically connect and update your security software.
- Protect all devices that connect to the Internet from all kinds of malware.
- Use your security software to scan all USBs and other external devices before attaching them to your computer.

Protecting your personal information:

- Secure your accounts with protection beyond passwords that can verify your identity before you conduct business.
- Make passwords long and strong with capital and lowercase letters, numbers, and symbols.
- Use different passwords for every account.
- Keep a list of your passwords stored in a safe place away from your computer.
- Use privacy and security settings to limit who you share information with.

Connecting with care:

- Delete any suspicious e-mail, tweets, posts, and online advertising.
- Limit the business you conduct from Wi-Fi hotspots and adjust your security settings to limit who can access your computer.
- Use only secure websites when banking and shopping, i.e., ones with **https://** or **shttp://** in their addresses.

Being web wise:

- Keep pace with new ways to stay safe online by checking trusted website for the latest information.
- Think before you act when you are implored to act immediately, offered something that sounds too good to be true, or asked for personal information.
- Back up your valuable information by making an electronic copy and storing it in a safe place.

Being a good online citizen:

- Practice good online safety habits.
- Post about others as you would have them post about you.
- Report all types of cybercrime to you local law enforcement agency and other appropriate authorities.